© THE QUEEN'S PRINTER FOR ONTARIO
2000

REPRODUCED WITH PERMISSION

L'IMPRIMEUR DE LA REINE POUR L'ONTARIO

REPRODUIT AVEC PERMISSION

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

A SPECIAL REPORT TO THE LEGISLATIVE ASSEMBLY OF ONTARIO ON THE DISCLOSURE OF PERSONAL INFORMATION BY THE PROVINCE OF ONTARIO SAVINGS OFFICE, MINISTRY OF FINANCE

April 26, 2000

Submitted by
Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION 3
  Background to the Complaint 3
  Events Surrounding the Privatization Initiative of the Province of Ontario Savings Office 4
  Issues Arising from the Investigation 5

RESULTS OF THE INVESTIGATION 5
  Issue A: Was the information in question "personal information" as defined in section 2(1) of the *Freedom of Information and Protection of Privacy Act* 5
  Issue B: Were the disclosures of personal information, a) from POSO to Privatization; b) from Privatization to Angus Reid; and c) from POSO to Wood Gundy, in compliance with section 42 of the *Act*? 6
  Issue C: Were reasonable measures taken with respect to the security of the account holder information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*? 19

SUMMARY OF CONCLUSIONS 25
  Final Comments 26

RECOMMENDATIONS 28
  Recommendations to the Ministry of Finance 28
  Recommendations to the Government of Ontario 29

ADDENDUM: Powers Necessary to Conduct a Proper Investigation

APPENDICES

A. List of individuals with whom interviews were requested; list of individuals interviewed;

B. *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 42, s. 52;

C. A Model Access and Privacy Agreement, IPC, August 1997;

D. Best Practices for Protecting Individual Privacy in Conducting Survey Research (Full Version), IPC, April 1999;

E. IPC's proposed amendments to Part IV of the *Freedom of Information and Protection of Privacy Act* provide for explicit powers and processes in relation to the investigation of complaints and review of compliance.

EXECUTIVE SUMMARY

On January 7, 2000, the Office of the Information and Privacy Commissioner (the IPC) decided to initiate an investigation into an incident involving account holders of the Province of Ontario Savings Office (POSO), which took place in 1997. The incident was brought to our attention by a reporter for *The Globe and Mail* on January 5, 2000.

The events examined in this Special Report were initiated by the Privatization Secretariat (Privatization), which was established by the Ontario Government to review government businesses and entities to determine if government involvement continued to be warranted. POSO was identified as a potential privatization candidate and a review of its operations was commenced.

In order to assist with this review, CIBC Wood Gundy (Wood Gundy) was retained by Privatization to provide financial analysis and advice. Privatization also contracted with the Angus Reid Group (Angus Reid) to survey POSO account holders, to evaluate their reaction to privatization. To facilitate this work, personal account holder information was provided to Privatization and the two firms.

Our investigation revealed that the information provided to Wood Gundy and Angus Reid included sensitive personal information such as the account numbers and account balances of POSO customers, their social insurance numbers, as well as their names and addresses. The information disclosed was far more detailed than was necessary or required. Both Wood Gundy and Angus Reid indicated that they did not need this level of detail in order to complete their contracted responsibilities. The IPC has concluded that the disclosures of account holder information from POSO to the Privatization Secretariat, from Privatization to Angus Reid, and from POSO to Wood Gundy, were not in compliance with the *Freedom of Information and Protection of Privacy Act* (the *Act*).

The investigation concluded that both Angus Reid and Wood Gundy handled the account holder information in a secure and responsible manner and took appropriate steps to ensure its confidentiality, while in their possession.

The Angus Reid survey project was abruptly terminated after numerous customer complaints were lodged with the Ministry of Finance in 1997, ultimately leading to the retrieval of the POSO account holder information. As a result of our investigation, the IPC has concluded that the bulk of the information has now been securely recovered.

The report's specific conclusions relating to the incidents in 1997 are as follows:

- The account holder information provided to Privatization, Wood Gundy and Angus Reid was "personal information" as defined in the *Act*;
- The three disclosures of personal information, (a) from POSO to Privatization, (b) from Privatization to Angus Reid, and (c) from POSO to Wood Gundy, were not in compliance with the *Act*;
- Reasonable measures were not taken with respect to the security of the information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*.

The report reviews the remedial steps taken by the Ministry of Finance, the ministry responsible for POSO, to address the confidentiality of personal information held by POSO. Seven recommendations were made, addressed to the Ministry, to help ensure that a similar incident of non-compliance with the *Act* does not occur in the future. These recommendations revolved around providing proper notice of collection, obtaining legal advice prior to the disclosure of personal information, conducting access and privacy training sessions, and ensuring that appropriate clauses, protective of privacy, are included in all contracts and consulting agreements.

Had the Ministry notified the IPC of the possible breach of the *Act* in 1997, this matter could have been dealt with quickly and expeditiously. This was the basis for our first recommendation to the Government: Upon learning of a possible incidence of non-compliance with the *Freedom of Information and Protection of Privacy Act*, a government organization should notify the Commissioner as quickly as possible.

The IPC has taken the extraordinary step of producing an Addendum to this report. The Addendum outlines the difficulties experienced by this Office in conducting the investigation into the disclosure of POSO account holder information. Prior to commencing the substantive investigation, the IPC was engaged by the Ministry of Finance in a series of discussions regarding our investigation process. In our view, the Ministry endeavoured to restrict the scope of the investigation and the investigative tools available to the IPC. Attempts to interview current and former government officials involved in the events of 1997 were met with protracted negotiations and resulted in key individuals refusing to be interviewed. The IPC has concluded that its duty to the Legislature and to the public to produce a comprehensive and timely report was hindered by the lack of clear, statutory power to investigate privacy breaches, as well as the lack of appropriate protections for witnesses.

The IPC recommends that the *Freedom of Information and Protection of Privacy Act* and its municipal counterpart be amended to include the explicit powers required to conduct proper and complete investigations into privacy matters. They include:

- the power to conduct investigations;
- the power to summons and examine witnesses under oath;
- the authority to order the production of records;
- the power to enter and inspect premises; and
- protections for witnesses giving evidence during an investigation.

Only through the introduction of these powers can the public be assured that the difficulties experienced by this Office will not be repeated in the future. The public deserves no less. In the end, privacy can only be protected in a comprehensive manner through the co-operation and concerted efforts of all those involved.

INTRODUCTION

Background to the Complaint

On January 5, 2000, the Office of the Information and Privacy Commissioner (the IPC) received a telephone call from a *Globe and Mail* reporter, describing an incident involving the Province of Ontario Savings Office (POSO) which took place in 1997.

On January 7, 2000, the Commissioner decided to initiate an investigation into the incident identified by the reporter. Following our past practice for investigations of this nature, we contacted the Ministry of Finance (the Ministry with responsibility for POSO).

On January 8, 2000, an article concerning the incident appeared on the front page of *The Globe and Mail*. It stated that during the summer months of 1997, the Ontario government's Privatization Secretariat had obtained account information from POSO and disclosed it to a polling firm. According to the article, the disclosed information included the names, addresses, telephone numbers and account balances of all POSO account holders. After receiving this information, the polling firm purportedly began calling these account holders to survey their views concerning the possible privatization of POSO. According to the article, these calls resulted in complaints made by various account holders to the government. The complaints centred on the fact that the polling firm had been given access to the account holders' confidential personal records. The survey was then abruptly stopped.

On January 10, 2000, the IPC placed a follow-up call to the Ministry of Finance, at which time we were informed that communications with the IPC would be handled through the Ontario Financing Authority. Later that day, we received a letter from the Secretary of Cabinet. She briefly outlined the events relating to the 1997 incident, explained that new procedures had been put in place to "address issues surrounding the disclosure of personal information," and invited further discussion.

On January 13, 2000, we held our first meeting with senior officials from the Ministry of Finance. Discussions revolved around the scope of our investigation. We asked for a complete chronology of the events which had taken place around the time of the 1997 incident. At this meeting we received our first assurance of full co-operation from the Ministry of Finance (the Ministry).

Initially, we contemplated two stages to our investigation. The first stage would deal with the security of the personal information that had been disclosed by POSO and would provide assurances to POSO account holders regarding the status of their personal information. The second part of the investigation would deal with the question of whether the disclosure in 1997 complied with the *Freedom of Information and Protection of Privacy Act* (the *Act*). Based on these initial discussions, we felt confident that the first phase of the investigation could be completed within a matter of weeks. During a January 14 appearance on Studio 2, a television public affairs program, the Commissioner made a commitment to release a public report by the end of January. Regrettably, we were unable to honour this commitment since information relating to this incident was only slowly forthcoming.

Beginning in mid-January, and continuing through February and March, it became increasingly clear that we would not be able to conduct a full and complete investigation. Our review was limited by the Ministry's initial challenge to our authority to conduct this investigation at all, efforts to limit its scope, and the reluctance or refusal of key individuals to be interviewed, including a number of current and former senior government s. (The accompanying Addendum outlines in detail the difficulties experienced by the IPC in conducting this investigation.)

Nonetheless, we have pieced together as best we can the events that occurred in 1997. While we do not have all of the information we feel we need, we are confident that this report will provide some answers to key issues under the *Freedom of Information and Protection of Privacy Act*.

Events Surrounding the Privatization Initiative of the Province of Ontario Savings Office

The Privatization Secretariat's mandate was to review government businesses and entities to determine if government involvement continued to be warranted. Each review was to incorporate expert advice and public input, including a consideration of various options. In 1997, the Privatization Secretariat (Privatization) identified POSO as a potential privatization candidate and commenced a review of its operations.

POSO was created in 1921 as a deposit-taking financial institution, providing banking services to the public through 23 branches and five agencies. POSO is currently operated by the Ontario Financing Authority (OFA), which is an agency of the Province of Ontario. The OFA is responsible for provincial borrowing and debt management activities and reports to the Minister of Finance through its Chair, who is also the Deputy Minister of Finance.

On May 23, 1997, Privatization released a Request for Proposal to select an advisor to assist in its review of privatization options for POSO. On July 7, Privatization announced that a contract had been awarded to CIBC Wood Gundy (Wood Gundy). A final report documenting the review of the privatization options and recommendations was due on August 13, 1997. Privatization also retained the Angus Reid Group (Angus Reid) to survey POSO customers regarding their views on various privatization options for POSO.

Documentation provided by the Ministry indicated that the following disclosures of POSO information took place during this time period:

(1) On July 16 or 17, 1997, POSO sent Privatization a CD-ROM containing the following information of all of its account holders: name, address, postal code, telephone number, social insurance number, client account number, account status, account balance, customer account information, language preference, residency, branch, June 1997 transactions, and all account features. Privatization returned the CD-ROM to POSO on July 18, 1997.

(2) On July 17 or 18, 1997, POSO sent Privatization a second CD-ROM containing the following information of account holders with telephone numbers: name, address, postal code, telephone number, social insurance number, account number, account status, account balance, language preference and branch.

(3) On July 23, 1997, Privatization sent this second CD-ROM to Angus Reid. Angus Reid returned this CD-ROM to POSO on or about August 20, 1997.

(4) On August 5, 1997, POSO sent Privatization a printout containing the following information of account holders from five branches: name, gender, account number, account type, balance, account status, high balance reason, last report date, recipient type, whether the customer banks elsewhere, and activity volume. Privatization returned the printout to POSO on August 20 or 21, 1997.

(5) On August 7 or 8, 1997, POSO sent Wood Gundy a CD-ROM containing the following information of all of its account holders: name, address, postal code, telephone number, social insurance number, account number, account balance, account status, language preference and branch. Wood Gundy returned this CD-ROM to POSO on August 19, 1997.

Issues Arising from the Investigation

The following issues were identified as arising from the investigation:

(A) Was the information in question "personal information" as defined in section 2(1) of the *Act*? If yes,

(B) Were the disclosures of information from a) POSO to Privatization; b) Privatization to Angus Reid; and c) POSO to Wood Gundy in compliance with section 42 of the *Act*?

(C) Were reasonable measures taken with respect to the security of the information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*?

RESULTS OF THE INVESTIGATION

Issue A: Was the information in question "personal information" as defined in section 2(1) of the *Freedom of Information and Protection of Privacy Act*?

Section 2(1) of the *Act* states, in part, that "personal information" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

M121

IMPORTANT NOTE CONCERNING THE FOLLOWING PAGES

THE PAGES WHICH FOLLOW HAVE BEEN FILMED TWICE IN ORDER TO OBTAIN THE BEST REPRODUCTIVE QUALITY

USERS SHOULD CONSULT ALL THE PAGES REPRODUCED ON THE FICHE IN ORDER TO OBTAIN A COMPLETE READING OF THE TEXT.

REMARQUE IMPORTANTE CONCERNANT LES PAGES QUI SUIVENT

LES PAGES SUIVANTES ONT ÉTÉ REPRODUITES EN DOUBLE AFIN D'AMÉLIORER LA QUALITÉ DE REPRODUCTION

LES UTILISATEURS DOIVENT CONSULTER TOUTES LES PAGES REPRODUITES SUR LA FICHE AFIN D'OBTENIR LA LECTURE DU TEXTE INTÉGRAL

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

...

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

There is no dispute that the information in question satisfies the requirements of the definition of "personal information" contained in one or more of paragraphs (a), (b), (c), (d) and (h) of section 2(1) of the *Act*. The Ministry's submissions agree with this conclusion.

Conclusion: The information in question was "personal information" as defined in section 2(1) of the *Act*.

Issue B: Were the disclosures of personal information, a) from POSO to Privatization; b) from Privatization to Angus Reid; and c) from POSO to Wood Gundy, in compliance with section 42 of the *Act*?

Facts Surrounding the Disclosures of Personal Information

From our review of the documentation and the interviews we conducted, there were several meetings and discussions which led up to the disclosure of personal information from POSO to Privatization, Privatization to Angus Reid, and POSO to Wood Gundy.

Privatization commenced a review of POSO's operations in 1997. Wood Gundy responded to a Request for Proposals issued by Privatization in June of 1997, and was successful in securing the contract to provide financial advice on the possible privatization of POSO. The contract between Wood Gundy and Privatization required Wood Gundy to provide advisory services for the period July 7 to September 1997. The terms of reference included identifying and assessing various options and making recommendations on privatization. Confidentiality considerations relating to this contract are discussed later in this report.

Wood Gundy stated that, after an initial meeting and over the course of the project, it specified to Privatization its information requirements. Wood Gundy did not request or require any personal information on individual POSO account holders. What Wood Gundy did require was anonymized information on POSO accounts, stratified into various pools according to account balances. The Ministry confirms that Wood Gundy only needed the data in aggregate form. This aggregate, non-identifying information was required to build a model of POSO operations in order to analyse different privatization scenarios. A series of back and forth discussions with Wood Gundy took place during the months of July and August, at times on a daily basis, attempting to obtain this aggregate information. These discussions began with Privatization but, for reasons of efficiency, eventually involved direct contact with POSO.

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

...

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

There is no dispute that the information in question satisfies the requirements of the definition of "personal information" contained in one or more of paragraphs (a), (b), (c), (d) and (h) of section 2(1) of the *Act*. The Ministry's submissions agree with this conclusion.

Conclusion: The information in question was "personal information" as defined in section 2(1) of the *Act*.

Issue B: Were the disclosures of personal information, a) from POSO to Privatization; b) from Privatization to Angus Reid; and c) from POSO to Wood Gundy, in compliance with section 42 of the *Act*?

Facts Surrounding the Disclosures of Personal Information

From our review of the documentation and the interviews we conducted, there were several meetings and discussions which led up to the disclosure of personal information from POSO to Privatization, Privatization to Angus Reid, and POSO to Wood Gundy.

Privatization commenced a review of POSO's operations in 1997. Wood Gundy responded to a Request for Proposals issued by Privatization in June of 1997, and was successful in securing the contract to provide financial advice on the possible privatization of POSO. The contract between Wood Gundy and Privatization required Wood Gundy to provide advisory services for the period July 7 to September 1997. The terms of reference included identifying and assessing various options and making recommendations on privatization. Confidentiality considerations relating to this contract are discussed later in this report.

Wood Gundy stated that, after an initial meeting and over the course of the project, it specified to Privatization its information requirements. Wood Gundy did not request or require any personal information on individual POSO account holders. What Wood Gundy did require was anonymized information on POSO accounts, stratified into various pools according to account balances. The Ministry confirms that Wood Gundy only needed the data in aggregate form. This aggregate, non-identifying information was required to build a model of POSO operations in order to analyse different privatization scenarios. A series of back and forth discussions with Wood Gundy took place during the months of July and August, at times on a daily basis, attempting to obtain this aggregate information. These discussions began with Privatization but, for reasons of efficiency, eventually involved direct contact with POSO.

At the same time, there were also discussions about different ways of gauging stakeholder reaction to the prospect of privatization and exploring the advantages and disadvantages of these options. It was decided that a customer survey would be conducted and that Angus Reid would do the survey. POSO stated that while these decisions were made by Privatization, POSO had provided information on a previous customer survey conducted by another polling firm in 1995. When a representative of POSO was asked during this investigation for details about the 1995 survey, he refused to respond due to concerns that the Ministry's waiver of his confidentiality oath did not extend to the incidents in 1995. In its submissions, the Ministry confirmed that an earlier survey of POSO customers had taken place in February of 1995. That survey was conducted by an outside consultant using a list of names and telephone numbers of customers who had recently visited a POSO branch.

The objective of the 1997 survey was to provide some indication to potential buyers of what customers would do if POSO was privatized. This was to support the work being done by Wood Gundy. The Angus Reid project started in late July and was to be completed by the beginning of September. The contract entered into between Angus Reid and Privatization was dated July 22, 1997.

A representative of POSO stated that discussions about Angus Reid's information needs took place between POSO and Privatization. POSO did not speak to Angus Reid directly prior to the personal information being disclosed. Instead, all discussions involving POSO took place with Privatization; Privatization then had direct discussions with Angus Reid. Angus Reid confirmed that this was the case.

POSO advised that after it learned about Angus Reid's needs through Privatization, it checked with its database service provider to see if the service provider could produce that information (since POSO does not administer its own database). In order to retrieve the desired information, POSO was advised that an extraction program had to be written and the speed at which one could retrieve information depended on whether a program already existed or could be modified. POSO did not then and does not now have the ability to extract data directly from its database.

POSO advised us that having determined what information was available, various options would have been discussed with Privatization. Privatization would have selected the option that most closely fit its content and time restrictions. Options providing less detailed information [while more privacy protective], would have taken more time (estimated at approximately two or three more weeks).

Angus Reid advised that the basic information needed to conduct a survey of this nature was the telephone numbers of POSO account holders [without names]. For this particular survey, Privatization asked Angus Reid to obtain feedback from a representative sample of account holders with different account balances. As a result, account holders needed to be divided into two pools – those account holders with balances under $60,000, and those with balances over $60,000. [The provincial government guarantees POSO balances over $60,000 which is the limit for deposits covered by the Canadian Depositors Insurance Corporation. As well, at POSO, balances over $60,000 attract a premium rate of interest.] Therefore, Angus Reid required two separate lists of telephone numbers to conduct the survey. Angus Reid clearly stated that the survey could have been conducted with this information alone – they did not require any personal client identifiers such as name, address, social insurance number, account number, account balance, or account status.

POSO advised that after discussing with Privatization the various options available, Privatization directed it to provide a CD-ROM containing detailed account holder information to Angus Reid, as this was the quickest solution. POSO had its outside service provider prepare the CD-ROM and then had it transferred to Privatization. Two CD-ROMs were sent to Privatization, however, one was in an unreadable format and had to be sent back to POSO. The second CD-ROM was the one that was eventually given to Angus Reid. POSO was unaware of whether Privatization had read it. In its submissions, the Ministry stated that Privatization did not access the data on the CD-ROM but conveyed the CD-ROM to Angus Reid. We were unable to confirm this because we could not interview anyone from Privatization. However, it appears likely that both CD-ROMs were accessed by Privatization or it would not have been able to determine that the first CD-ROM was not in readable format, but the second CD-ROM was readable.

Angus Reid received the CD-ROM via courier from Privatization in late July. The CD-ROM contained more than 50,000 accounts, apparently comprising the entire database of POSO account holders. According to information provided by the Ministry, this CD-ROM was obtained by Privatization from POSO on July 17 or 18, and then passed on to Angus Reid on July 23, 1997. It contained the following information of all account holders with telephone numbers:

(1) name
(2) address
(3) social insurance number
(4) telephone number
(5) account number
(6) account balance
(7) account status
(8) POSO branch
(9) language preference

Angus Reid confirmed that it had received this type of information. Angus Reid then imported this information from the CD-ROM into a spreadsheet and edited it for use in the survey. Duplicate names, inactive accounts, and large institutional depositors were deleted. By sample management, the number of account holders was reduced to approximately 31,000, and then sorted by account balance from high to low. Angus Reid took the accounts with balances in excess of $60,000 and placed them on a separate spreadsheet. All information from both spreadsheets was then deleted, with the exception of the telephone numbers. The two groups of telephone numbers were sent to the Angus Reid field office in Winnipeg via internal company e-mail. Only one employee at Angus Reid had access to the CD-ROM. Once the information contained on the CD-ROM was stratified for survey purposes, this employee locked it securely in his desk drawer.

Angus Reid advised that it had anonymized POSO account holder information on its own initiative and did not recall having any discussions with Privatization as to whether or not this was appropriate. Angus Reid said it had received far more information than was required to actually perform the survey.

In its submissions, the Ministry states the reason that the CD-ROM was transferred to Angus Reid was that the information systems of POSO and Privatization lacked the technical capability to segregate the accounts into those balances over and under $60,000 and to generate lists of names and telephone numbers only based on that information.

Angus Reid advised that the spreadsheets it created were saved in a computer directory that was accessible by approximately six employees. None of these employees had direct access to the actual CD-ROM. The survey was conducted between August 8 to 17, 1997. Angus Reid confirmed that survey interviewers did not have access to any personal information other than the telephone numbers which were stored in the computer and fed electronically to the interviewers as the calls were made. The interviewers did not necessarily know whether the person they were contacting belonged to the high or low-deposit group. Interviewers recorded numeric and verbatim responses to the set of questions asked. According to Angus Reid, a survey of this size required between 30 to 40 interviewers.

In its submission, the Ministry states that the CD-ROM that was transferred to Angus Reid was seen by only one employee. Contrary to Angus Reid's recollection, the Ministry states that the names and telephone numbers of the sample group of account holders were used by interviewers for the purpose of the survey. To clarify exactly what information was given to interviewers, we tried to interview some of the interviewers who had worked on this survey. Unfortunately, we were told that the interviewers were no longer employed by Angus Reid since the office had been closed and moved to another city.

In the meantime, Wood Gundy states that POSO was unable to provide the information requested by it in the required format. In its submissions, the Ministry confirms that this was the case because, again, POSO was unable to produce the requisite data using its own information systems. A representative of POSO stated that POSO staff reviewed the options available for providing the required information to Wood Gundy with Privatization. The quickest option for fulfilling Wood Gundy's request was to provide a CD-ROM (similar to that given to Angus Reid), prepared by the outside service provider, containing detailed account holder information. POSO advises that it was instructed by Privatization to pursue this option.

On or about August 7 or 8, 1997, POSO provided Wood Gundy with a CD-ROM apparently containing all POSO account holder information.

Wood Gundy staff had the impression that they were given the entire database of POSO account holder information. According to the information provided by the Ministry, the CD-ROM provided by POSO to Wood Gundy contained the following information for all account holders:

(1) name
(2) address
(3) social insurance number
(4) telephone number
(5) account number and status
(6) account balance
(7) POSO branch
(8) language preference

Wood Gundy confirmed that this was the type of information it had received.

A summer student at Wood Gundy, assisted by an analyst, was given the task of transferring the information on the CD-ROM into a format that could be used. This was accomplished by extracting the information from the CD-ROM and importing it into an Excel file format on multiple spreadsheets. The summer student and analyst required some technical assistance from one other person in order to complete this task. The information was stored on the hard disk of at least one personal computer and on the computer network to which the six employees in the group plus the necessary technology infrastructure group at Wood Gundy had access. The newly created information consisted of aggregate data which was incorporated into a report submitted to Privatization in September of 1997.

While at Wood Gundy, the information was securely stored in accordance with its strict internal requirements. As well, no one employee would have had access to another employee's password-protected personal computer.

Documents and interviews establish that Privatization had contacted the Ministry's Freedom of Information and Privacy Co-ordinator (the Co-ordinator) on or about July 28, 1997. The Co-ordinator was asked whether the disclosure of personal information to Angus Reid for the purpose of conducting the survey was in compliance with the *Act*. He said that it was. However, a number of troublesome points remain:

(1) the documents showed, and the Co-ordinator confirmed, that his advice was sought and received *after* the CD-ROM had been given to Angus Reid;

(2) even though the exact amount of personal information disclosed to Angus Reid was not made clear to him, the Co-ordinator advised Privatization that too much information had been given to Angus Reid;

(3) according to the Co-ordinator, he had not been provided with any documents to review;

(4) the advice sought from the Co-ordinator applied only to the disclosure to Angus Reid but not to Wood Gundy.

The Ministry states that the Co-ordinator spoke to legal counsel with the Ministry's Legal Services Branch on July 28, 1997 to discuss compliance with the *Act*, but that no written legal opinion was requested or received. There is no evidence that a legal opinion was obtained by Privatization or POSO prior to disclosing the CD-ROM to Angus Reid. However, a short written legal opinion was prepared by Ministry counsel on August 20, 1997, after the disclosures to both Angus Reid and Wood Gundy had taken place, and after the information contained on the CD-ROMs had been used by these two organizations. This legal opinion did not address the disclosure of personal information to Wood Gundy, only the disclosure to Angus Reid.

On July 29, 1997, Privatization asked Angus Reid for written assurances on how the data would be used, which Angus Reid then provided. Angus Reid was not advised of the requirements of the *Act* or given any information about it. Nor was Angus Reid required to sign a non-disclosure agreement specifically relating to the personal information received during this assignment. We will discuss the adequacy of the contract in greater detail later in this report.

A representative of POSO stated that verbal assurances had been received from Privatization staff that the appropriate contractual clauses were in place with Angus Reid to safeguard the sensitive information given to them. In addition, POSO stated that Privatization claimed to have received the appropriate approvals for disclosing the information. In essence, POSO relied upon Privatization to deal with questions of disclosure and confidentiality. We were unable to confirm this with representatives of Privatization and, as a result, we do not know what steps may or may not have been taken in this regard.

Angus Reid confirmed that it completed the survey and prepared detailed tables analysing the results. However, unlike most survey assignments of this nature, no final report was prepared, nor was a presentation made to the client. Angus Reid recalls receiving a telephone call from Privatization in mid-August, directing it to immediately stop work on the project. No reasons were provided.

Angus Reid was aware that three or four complaints had been received from POSO account holders contacted during the survey. The complaints were made directly to POSO branch managers, not to Angus Reid. Angus Reid has no knowledge of how they were handled. The documents provided by the Ministry indicate that complaints were received by 12 branches, with one branch reporting approximately 30 complaints. The complaints included: 1) the fact that account holders were called; 2) that fact that someone had been given account holders' telephone numbers; 3) account holders' dislike of the questions asked; 4) interviewers' knowledge of account holders account numbers; and 5) interviewers' knowledge of their substantial bank balances.

Retrieval of Information

POSO could not provide us with any details surrounding the return of the CD-ROM given to Angus Reid. According to Angus Reid, POSO asked that the CD-ROM be returned personally rather than by courier, which Angus Reid did on or about August 20, 1997. Angus Reid advised that discussions concerning the return of the CD-ROM was the only time it recalls having spoken directly with POSO officials; all other discussions had been with Privatization. The steps taken by Angus Reid to safeguard and return the personal information were then documented in writing and sent to both Privatization and POSO on August 19, 1997.

Ministry documents indicate that the original CD-ROM which Wood Gundy received from POSO was returned to POSO on August 19, 1997, after several complaints had been received from POSO account holders about the Angus Reid survey. The return date also coincides with the then-Deputy Minister of Finance becoming aware that the information had been provided to Angus Reid. Staff at Wood Gundy confirmed that it had been returned after only a few days in their possession but were unable to confirm specific details regarding the means of return of this CD-ROM.

According to a government auditor who conducted a review of the disclosure incidents, a second CD-ROM thought to be created by Wood Gundy was retrieved by him on August 25, 1997 and remains securely stored in his office.[1] Wood Gundy was unable to confirm this since it did not recall having created the second CD-ROM, nor having any involvement with the government auditor.

---

[1] Given that the Auditor has no further use for this CD-ROM, we suggest that it be returned to POSO as soon as possible.

Wood Gundy confirmed to us that any and all personal information stored on computer hard disks had been deleted. A file scan confirmed that none of these files are currently on its computer system. During the course of our investigation, we asked Wood Gundy to check its network backups to ensure that all of the personal information from the CD-ROM had been deleted. Wood Gundy stated that it is required to maintain a network backup, which is stored off-site. This backup happens to contain the personal information from POSO, together with information required to be retained for regulatory and audit purposes. Wood Gundy advised this information is kept in an off-site secure location for a seven-year period. Wood Gundy confirmed that there was also some personal information on its in-house network backups, however, it advised that it has now deleted all such in-house information.

In his August 25, 1997 report, the government auditor concluded that, "Wood Gundy was given far more data than it required or had requested, all of it of a confidential nature." We are led to the same conclusion. Although the Co-ordinator's advice was sought with respect to the disclosure to Angus Reid, neither he nor any lawyer appears to have been consulted by either POSO or Privatization regarding the disclosure of POSO account holder information to Wood Gundy. We have also received nothing to indicate that either POSO or Privatization took privacy considerations or the provisions of the *Act* into account at the time decisions were made to disclose the account holder information to Wood Gundy. Similarly, we have nothing to indicate that any internal discussions took place at that time among individuals in the Privatization Secretariat or elsewhere in government about the advisability of making these disclosures.

Based on our discussions with Angus Reid and our review of the information provided by the Ministry, we are satisfied that Angus Reid handled the account holder information in an appropriate manner and with due care, given its sensitive and confidential nature. On its own initiative, Angus Reid took steps to ensure that any information identifying account holders other than telephone numbers was deleted from its spreadsheet files and not made available to other Angus Reid employees and was not used for the purpose of conducting the telephone survey. A representative of Angus Reid confirmed that he personally returned the CD-ROM to POSO on or about August 20, 1997. Angus Reid also confirmed that all of the information that it received from POSO for this survey has been destroyed or overwritten on its network servers. As a result, we are satisfied that all the information given to Angus Reid has been returned to POSO.

We are also satisfied that the account holder information disclosed by POSO to Wood Gundy was handled appropriately by Wood Gundy. The bulk of this information was later securely recovered by both POSO and the government auditor involved.

After receiving a draft copy of this report, the Ministry submitted that both the report and the 1997 internal Management Board Secretariat audit confirmed that, in the Ministry's words, "information on account holders was never in the hands of anyone other than staff or those acting with integrity on our behalf." We have not reached this conclusion nor can we find such a statement in the Auditor's report. While we are satisfied with the way in which Wood Gundy and Angus Reid handled the information disclosed to them, we are unable to substantiate so broad a conclusion without the benefit of interviewing all key players.

Section 42 Analysis

Section 42 of the *Act* sets out the rules for the disclosure of personal information other than to the individual to whom the information relates. This section provides that an institution shall not disclose personal information in its custody or under its control, except in the circumstances listed in sections 42(a) through (n) (see Appendix B for full text). The Ministry has also raised the permitted use provisions at section 41 of the *Act*. For the purpose of our analysis, the pertinent provisions of the *Act* at issue are set out below:

> **41.** An institution shall not use personal information in its custody or under its control except,
>
> (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
>
> (c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*.
>
> **42.** An institution shall not disclose personal information in its custody or under its control except,
>
> . . . . .
>
> (b) where the person to whom the information relates has identified that information in particular and consented to its disclosure;
>
> (c) for the purpose for which it was obtained or compiled or for a consistent purpose;
>
> (d) where disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions;
>
> **43.** Where personal information has been collected directly from the individual to whom the information relates, the purpose of a use or disclosure of that information is a consistent purpose under clauses 41(b) and 42(c) only if the individual might reasonably have expected such a use or disclosure.

The Ministry claims that none of the transfers of personal information from POSO to Privatization, from Privatization to Angus Reid, and from POSO to Wood Gundy, was a "disclosure" within the meaning of section 42 of the *Act*. Instead, the Ministry submits that each such transfer was a "use" of the information authorized by section 41 of the *Act*. In making this submission, the Ministry relies on the following facts: (1) that the disclosure from POSO to Privatization was within the same institution, i.e., the Ministry; and (2) that the disclosures by Privatization to Angus Reid and by POSO to Wood Gundy were to contractors retained to assist Privatization in making an assessment and recommendation on the question of privatizing POSO.

While we accept that the information transferred was used for the purposes of assessing the viability of privatizing POSO and canvassing the views of POSO's customers on privatization, this does not mean that the information was not also "disclosed" in the course of these transfers or in furtherance of these uses. In our view, each transaction was clearly a disclosure within the meaning of the *Act* and cannot be viewed otherwise under the statute.

Section 42(d) of the *Act* makes it clear that the disclosure of personal information within an institution is considered to be a disclosure which must be justified in each case. Disclosure of personal information can only be made to "an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions."

There would be no need for the Legislature to have enacted such a provision if disclosure within an institution were not considered a "disclosure" within the meaning of section 42. Indeed, section 42(d)'s dual requirements – that the employee must need the record in the performance of his or her duties and that disclosure must be a necessary and proper part of the institution's functions – underscores the Legislature's unambiguous objective that disclosure of personal information within an institution should be subject to scrutiny on a "need to know" basis. This, of course, is not to say that disclosure is not permitted to be made to persons outside of an institution; most of the remaining exceptions to the prohibition contemplate circumstances where such disclosure is not only permitted, but desirable to achieve other legitimate government objectives. However, it is clear that disclosure of information within an institution is considered not simply to be a "use," for the reason only that it is internal and not external. An internal disclosure must be justified in accordance with the requirements of section 42.

Accordingly, we find that each of the transfers of personal information from POSO to Privatization were disclosures within the meaning of the *Act*.

The Ministry also submits that neither the transfer from Privatization to Angus Reid nor the transfer from POSO to Wood Gundy constituted a "disclosure" within the meaning of section 42. Again, the Ministry states that each such transfer is a "use" within the meaning of section 41 of the *Act*. The Ministry relies on a July 1997 Management Board Secretariat (MBS) Bulletin and accompanying draft paper which states that where custody or control of records is maintained by an institution, the transfer of the information to an Alternative Service Delivery (ASD) provider is considered only to be a "use" of personal information, and that the disclosure provisions of the *Act* do no apply. The Ministry suggests that the IPC has endorsed the legal position set out in the MBS bulletin and in an accompanying draft paper. The Ministry purports to rely on an IPC paper entitled, "Model Access and Privacy Agreement,"(Appendix C) dealing with transfers of government services to ASD providers in cases where government does **not** retain custody or control of the records.

The IPC's position on the issue of "use" versus "disclosure" is set out in Investigation Report I97-017P, released the same month as the MBS bulletin and also referred to in the IPC "Model Agreement" paper. This report deals with the transfer of personal information connected with the administration of social welfare assistance by MBS to a collection agency performing the ASD function of debt collection on the government's behalf. The records in that case were clearly under the control of MBS or we would not have investigated the matter and made a finding on compliance with the *Act*. Indeed, the IPC recommended that the ASD agreement when renewed, should be amended to include a specific provision acknowledging that the records remained under the control of MBS. The report dealt with and disposed of the issues on the basis that the transfer of personal information to the collection agency was a "disclosure" under the *Act*, albeit one permitted by section 42(c) in the particular circumstances of that case.

Accordingly, even if it could be argued that Angus Reid and Wood Gundy were retained as ASD providers to deliver traditional government services (a position which we do **not** accept), rather than simply as advisory consultants in a particular case, Investigation Report I97-017P makes it eminently clear that the transfer of personal information in such a case involves the disclosure of personal information, not just its use. We fail to see how the Ministry can assert that the IPC has endorsed a different view.

The principal questions raised in this investigation, therefore, remain the ones posed in our invitation to the Ministry to make submissions: whether the "disclosures" we have identified were permitted by section 42 of the *Act*.

While the Ministry's submissions in this respect are made primarily in relation to the "use" provisions of sections 41(b) [purpose for which compiled] and 41(c) [purpose permitted by section 42(d)], essentially the same arguments are relied upon to support the Ministry's contention that POSO's disclosure to Privatization was permitted by sections 42 (c) and (d) of the *Act*, and that the disclosures by POSO to Wood Gundy and by Privatization to Angus Reid were permitted by section 42(c) alone.

The Ministry submits that each of the disclosures was in compliance with section 42(c) since disclosure was "for the purpose for which it was obtained or compiled or for a consistent purpose." In support of this submission, the Ministry argues that POSO customers "might reasonably have expected such a use or disclosure" within the meaning of section 43 of the *Act*.

In our view, POSO collected the personal information at issue for the purpose of administering its customers account deposits, the core of its business activity, and for no other purpose. While it is to be expected, as the Ministry submits, that POSO should seek "to operate efficiently and effectively in the interests of its customers and the taxpayers of Ontario," we cannot accept that this is the very reason for collecting customer account information. Unlike the circumstances of Investigation Report I97-017P, the various disclosures of personal information to Privatization, Angus Reid and Wood Gundy, for the purpose of assisting Privatization's review of POSO operations and exploring the possibilities of privatization, were not for the same purpose for which the information was obtained or compiled by POSO.

We also find that these disclosures were not for a "consistent purpose" within the meaning of section 42(c). In our view, POSO customers would not have had a reasonable expectation that their personal account information would be disclosed to any of these entities for a purpose which, at best, is only remotely connected with the provision of banking services by POSO.

Previous investigation reports of this Office have stated that the reasonableness of an expectation of disclosure should be assessed at the initial time the personal information is collected from the individual (see I96-051P). In one case, we determined that disclosure of personal information for a customer survey connected with the larger business or operational purposes of an institution, and not with the immediate concerns of the individual supplying the information, would only have been "reasonably expected" if the individual had been informed at the outset that the institution might do this (I98-014P). On the other hand, where information was collected pursuant to a notice of collection which stated that it would be used for the institution's "planning and co-ordination" purposes, disclosure for the purposes of a related planning survey was considered to be within the reasonable expectations of the individuals to whom the information related (I93-059P).

In addition, the existence of an economic or similar interest in the personal information by another entity has been considered to be insufficient, standing alone, to infer a reasonable expectation that the information would be disclosed to that other entity (I95-096P). Finally, even if it could be said that some measure of disclosure is for a consistent purpose, this only extends to the type and amount of information necessary to fulfil that other purpose. Individuals would not reasonably expect that more personal information than was necessary would be disclosed to fulfil a purpose other than the one for which the information was collected (I93-046P).

In the case at hand, a letter from the OFA's CEO, dated April 28, 1997, was available in POSO branches to be given to customers if they had any questions or concerns about the situation. This letter brought to their attention the fact that the government was looking into various options for improving efficiency, including divestiture. In our view, this is not sufficient to form the basis for customers to expect that their personal account information would be shared with other persons or outside entities, for this or any other purpose. Moreover, the fact that this letter was not sent but merely made available to customers, in the event that they had any questions or concerns, essentially renders this communication ineffectual. It also begs the question of how account holders would know of the existence of such a letter – a necessary prerequisite to be in a position to ask for it.

Merely because Privatization may have had an interest in securing this information and using it for the purposes specified, or that POSO may have had a parallel interest in disclosing it, cannot lead to a reasonable expectation among customers that their personal information will be used for those purposes. If it were otherwise, then whenever government formulated a social or economic objective for using or disclosing personal information, we would be required to impute a reasonable expectation among individual members of the public consistent with those objectives. Such a view of the operation of the privacy provisions of the *Act* would render their protections meaningless and frustrate the important legislative objectives set out in the purpose clause of the *Act* and in section 42.

It appears that the only notice of the purpose of the collection of their personal information that was given to POSO customers occurred by way of the posting in branch offices of a document entitled "Freedom of Information and Protection of Privacy Act" which had been distributed to Branch Managers by POSO Head Office under a covering memorandum dated March 9, 1990. The full text of this document states:

> Certain personal information such as name, address, social insurance number and details of financial transactions is collected by the Province of Ontario Savings Office under authority of the Agricultural Development Finance Act, R.S.O. 1980,

> c 10. This information is used to administer such financial services as savings accounts, handling of securities and other financial paper.
>
> All personal information held by the Province of Ontario Savings Office is protected from unauthorized access by the Freedom of Information and Protection of Privacy Act, 1987.
>
> Customers requiring information about the operation of these acts should consult the branch manager.

We consider the simple posting of "purpose of collection" notices on the premises of institutions to be inadequate, as there is no way of assuring that the notice is actually brought to the attention of the individuals to whom it relates. Nonetheless, to the extent that this document provides notice of the purpose of the collection, that purpose is clearly related to the administration of savings accounts and related banking services. No additional notice of the purpose of the collection appears to have been given to POSO customers at the time the information was collected, whether at the point when accounts were opened, when account information was changed, or when account transactions were conducted. Additionally, there is no other indication that customers might have reason to expect that their personal information would be used for anything other than banking and transactional purposes.

We were also provided with a revised notice of purpose of collection document dated March 13, 2000 (two months after the date this investigation commenced), the full text of which reads as follows:

> Personal Information such as customer names, account numbers, addresses, social insurance numbers, telephone numbers and details of financial transactions is collected by the Province of Ontario Savings Office under the legal authority of the Province of Ontario Savings Office Act, R.S.O. 1990 and the Capital Investment Plan Act, 1993, S.O. 1993, c. 23.
>
> This information is used to administer customer accounts, safety deposit boxes, and to administer and control records associated with the purchase and sale of financial papers. Account information and interest paid to clients is reported to Revenue Canada as required by the Income Tax Act. Account information may also be used for contacting customers regarding Savings Office products or services or for conducting financial and marketing research and analysis regarding POSO.
>
> All personal information held by POSO is subject to the Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31
>
> Customers requiring information about the collection of personal information should consult the Regional Manager, 33 King Street West, 6th Floor, Oshawa Ontario L1H 8H5, 1-888-283-8333.
>
> (Revised Version, March 13, 2000)

While an improvement on the previous notice, we have concerns that this revised notice (which appears to be in the form of a posting) is also insufficient to give rise to a reasonable expectation among existing customers of any non-banking service purposes for which their personal information may now be intended to be used or disclosed. As we have said, the reasonableness of such an expectation should be considered at the time the information was collected; it cannot be imputed after the fact by notice of other purposes that may later be contemplated. Customers are entitled to govern their financial affairs, and to rely upon and act on the basis of information available to them at the time they provide their personal information. Accordingly, we do not find that this revised notice is now sufficient under the consistent purpose provisions of section 42(c) to permit any of the disclosures that occurred in this case in relation to existing customers with current deposits on account with POSO. Moreover, to the extent that the terms of this notice may be sufficient to give notice to new or future customers, or even to existing customers with the passage of time, we consider a posting in the branch to be less than adequate notice and would recommend that such notices be incorporated into banking forms or mailings and provided to customers on an individual basis. There would appear to be no administrative obstacles to doing this.

The Ministry also submits that it was not inappropriate for POSO to use an outside service provider to process account holder information on its behalf, and that its relationships with Wood Gundy and Angus Reid were of a similar nature. The implication is that the disclosures to Wood Gundy and Angus Reid should also be considered to be appropriate because these organizations are also outside service providers to POSO. We do not believe that this analogy advances the Ministry's position.

Banking customers understand that their account transactions must be administered and processed for obvious record-keeping purposes. It makes no difference to customers if this work is performed "in-house" by persons employed directly by the bank, or by employees of an outside service provider, provided that the same rules govern the confidentiality and security of their information in either setting. In the POSO setting, disclosure to the outside service provider was for the very purpose for which the information was collected – the administration and processing of account transactions – and was therefore permitted under section 42(c). (See Investigation Report I97-017P.) The pertinent distinction is that the disclosures to Wood Gundy and Angus Reid were not for the same purpose for which the information was obtained or compiled, nor for a consistent purpose.

Following along these lines, section 42(c) does not operate to impede the alternative delivery of government services where this entails the transfer of personal information; but neither does it permit disclosure to outside entities for other reasons of perceived government expediency. If government was permitted to disclose personal information to outside service contractors based solely on its perceptions of what might be most expedient in the circumstances, and regardless of the purpose of the original collection or the expectations of the individuals involved, privacy rights in Ontario would be seriously eroded.

In all of the circumstances involved in this case, the proper way for POSO and Privatization to have proceeded in 1997 would have been for POSO: (1) to have restricted the disclosure of personal information to Angus Reid, only to that which was necessary for the purpose of conducting the survey (i.e., a sample of telephone numbers divided according to accounts over and under $60,000); **and** (2) to have obtained from customers their explicit and informed consents to the disclosure of this personal information, pursuant to section 42(b) of the *Act*, before such disclosures occurred.

M121

IMPORTANT NOTE CONCERNING THE FOLLOWING PAGES

THE PAGES WHICH FOLLOW HAVE BEEN FILMED TWICE IN ORDER TO OBTAIN THE BEST REPRODUCTIVE QUALITY

USERS SHOULD CONSULT ALL THE PAGES REPRODUCED ON THE FICHE IN ORDER TO OBTAIN A COMPLETE READING OF THE TEXT.

REMARQUE IMPORTANTE CONCERNANT LES PAGES QUI SUIVENT

LES PAGES SUIVANTES ONT ÉTÉ REPRODUITES EN DOUBLE AFIN D'AMÉLIORER LA QUALITÉ DE REPRODUCTION

LES UTILISATEURS DOIVENT CONSULTER TOUTES LES PAGES REPRODUITES SUR LA FICHE AFIN D'OBTENIR LA LECTURE DU TEXTE INTÉGRAL

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

As we have noted earlier, anonymous aggregate information was clearly all that Wood Gundy required; thus it was unnecessary for any personally identifiable information to have been disclosed to Wood Gundy. If POSO and Privatization had only provided aggregate information, then no issue of disclosure under section 42 of the *Act* would have arisen. While informed customer consent would also have ensured compliance with section 42 pursuant to paragraph (b), the disclosure of any personal information to Wood Gundy clearly cannot be justified on the basis of any need for this information or consistency with the purpose of the original collection.

We refer the Ministry to the IPC's April 1999 paper entitled "Best Practices for Protecting Individual Privacy in Conducting Survey Research," (Appendix D) on the conduct of survey research in general, and in particular, on the advisability of providing adequate notice of the purpose of a collection and other potential uses or disclosures, and of securing appropriate consent to an inconsistent use or disclosure.

Finally, with reference to the Ministry's reliance on section 42(d) to justify POSO's disclosure to Privatization, the evidence shows that employees of Privatization did not require any of this information for any purpose whatsoever. Privatization merely passed along the CD-ROM to Angus Reid, we were told, without examining or otherwise using it in any way except to replace an unreadable disk. To the extent that this amount of information needed to be disclosed to Angus Reid (a proposition which we do not accept), it was clearly not necessary for Privatization to intervene as a conduit and have access to the information in both printed and electronic form in order to accomplish this purpose. The fact that an employee within Privatization was generally charged with the responsibility for co-ordinating the POSO review does not mean that he/she should have access to personal information where this is not "necessary and proper in the discharge of the institution's duties" and he/she does not "need the record in the performance of his or her duties." As with the transfer of the CD-ROM directly from POSO to Wood Gundy, the intervention of Privatization was not necessary to effect any purpose associated with the Ministry's functions or to facilitate any of the duties of the individual who received the CD-ROM on Privatization's behalf.

Conclusion: The three disclosures of personal information, (a) from POSO to Privatization, (b) from Privatization to Angus Reid, and (c) from POSO to Wood Gundy, were not in compliance with the *Act*.

Issue C: Were reasonable measures taken with respect to the security of the account holder information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*?

We wish to emphasize at the outset of this discussion that measures taken by an institution to ensure the security and confidentiality of personal information do not necessarily have any bearing on the issue of whether or not disclosure of the information was in compliance with section 42(c) and (d) of the *Act*. Unless disclosure is permitted in one or more of the circumstances set out at paragraphs (a) to (n) of section 42, no amount of confidentiality protection by contract or otherwise will save an impermissible disclosure from a finding of non-compliance.

As we have noted earlier, anonymous aggregate information was clearly all that Wood Gundy required; thus it was unnecessary for any personally identifiable information to have been disclosed to Wood Gundy. If POSO and Privatization had only provided aggregate information, then no issue of disclosure under section 42 of the *Act* would have arisen. While informed customer consent would also have ensured compliance with section 42 pursuant to paragraph (b), the disclosure of any personal information to Wood Gundy clearly cannot be justified on the basis of any need for this information or consistency with the purpose of the original collection.

We refer the Ministry to the IPC's April 1999 paper entitled "Best Practices for Protecting Individual Privacy in Conducting Survey Research," (Appendix D) on the conduct of survey research in general, and in particular, on the advisability of providing adequate notice of the purpose of a collection and other potential uses or disclosures, and of securing appropriate consent to an inconsistent use or disclosure.

Finally, with reference to the Ministry's reliance on section 42(d) to justify POSO's disclosure to Privatization, the evidence shows that employees of Privatization did not require any of this information for any purpose whatsoever. Privatization merely passed along the CD-ROM to Angus Reid, we were told, without examining or otherwise using it in any way except to replace an unreadable disk. To the extent that this amount of information needed to be disclosed to Angus Reid (a proposition which we do not accept), it was clearly not necessary for Privatization to intervene as a conduit and have access to the information in both printed and electronic form in order to accomplish this purpose. The fact that an employee within Privatization was generally charged with the responsibility for co-ordinating the POSO review does not mean that he/she should have access to personal information where this is not "necessary and proper in the discharge of the institution's duties" **and** he/she does not "need the record in the performance of his or her duties." As with the transfer of the CD-ROM directly from POSO to Wood Gundy, the intervention of Privatization was not necessary to effect any purpose associated with the Ministry's functions or to facilitate any of the duties of the individual who received the CD-ROM on Privatization's behalf.

Conclusion: The three disclosures of personal information, (a) from POSO to Privatization, (b) from Privatization to Angus Reid, and (c) from POSO to Wood Gundy, were not in compliance with the *Act*.

Issue C: Were reasonable measures taken with respect to the security of the account holder information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*?

We wish to emphasize at the outset of this discussion that measures taken by an institution to ensure the security and confidentiality of personal information do not necessarily have any bearing on the issue of whether or not disclosure of the information was in compliance with section 42(c) and (d) of the *Act*. Unless disclosure is permitted in one or more of the circumstances set out at paragraphs (a) to (n) of section 42, no amount of confidentiality protection by contract or otherwise will save an impermissible disclosure from a finding of non-compliance.

Section 4 of Regulation 460 states in part:

> 4.– (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.
>
> (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
>
> ...

In order to determine whether adequate safeguards were in place to protect the personal information provided to Angus Reid and Wood Gundy, we reviewed the contractual agreements entered into between these two organizations and Privatization, as well as several other documents provided by the Ministry, such as standing agreements and guidelines, and communications dealing specifically with the confidentiality issues arising in this case.

In reliance on this material, the Ministry submits that there were various general policies and procedures in place and numerous specific steps taken at the time of the Angus Reid survey in August 1997, designed to ensure the confidentiality of personal information generally and/or for the purpose of the Angus Reid survey in particular.

The Ministry advises that the general policies and procedures in place at the time of the survey included the following:

(1) The Operational Procedures Manual used by POSO at that time, which contained a general prohibition against the release of POSO customer account information other than to the account holder, his or her authorized representative or as required by law.

(2) A June 1995 "Information and Privacy Bulletin" issued by the Ministry of Finance which attached "Suggested Terms for Use in Contracts Dealing with the Disclosure of Personal Information."

(3) A "Standing Agreement for Commissioned Opinion Research Services" between the Crown and Angus Reid, dated February 1, 1996.

(4) "Standing Guidelines for Advisory Services Requests for Proposals" dated May 20, 1997.

The Ministry advises: (1) that the Standing Agreement referred to at item 3 contained both a confidentiality provision and a specific section reciting that the Standing Agreement is governed by the *Act*; and (2) that the Standing Guidelines referred to at item 4 also contained confidentiality provisions.

The Ministry also advises that specific steps taken to ensure the confidentiality of the personal information in the Angus Reid survey included the following:

(1) The April 28, 1997 letter from OFA's CEO advising customers that there would be a review of the operations of POSO conducted by Privatization and "supported by a panel of impartial experts and a variety of processes to ensure input from employees and the public." (As noted earlier, however, this letter was not sent but merely made available to customers, upon request.)

(2) The July 22, 1997 Agreement between Privatization and Angus Reid which contained a "confidentiality" clause and incorporated the Standing Guidelines by reference.

(3) On July 28, 1997, Privatization sought further assurances from Angus Reid as to how the information on the CD-ROM would be handled. By memorandum dated July 29, 1997, Angus Reid confirmed that it would handle the information confidentially.

(4) At the same time, Privatization sought and obtained verbal assurance from the Ministry's Freedom of Information and Privacy Co-ordinator that its actions were not in contravention of the *Act*. The Freedom of Information and Privacy Co-ordinator also recalls discussing the matter with a senior legal adviser with the Ministry on July 28, 1997.

(5) On July 31, 1997, the Freedom of Information and Privacy Co-ordinator briefed the staff of Privatization on the requirements of the *Act* and confirmed that the use of the information was consistent with the *Act*.

POSO's obligations under the *Act* with respect to the use and disclosure of its account holders' personal information flow from the fact, which is not in dispute, that the records containing the information, the CD-ROMs and the printout, were at all material times either "in the custody" or "under the control"of POSO within the meaning of sections 41 and 42 at Part III of the *Act*.

In any circumstance contemplating the transfer of personal information into the hands of third parties engaged to perform services on the government's behalf, all of the privacy protections under the *Act* must be respected and, if necessary, secured by contract. Similar requirements are described in the IPC's published papers, "A Model Access and Privacy Agreement" (August 1997), and "Best Practices for Protecting Individual Privacy in Conducting Survey Research (Full Version)," (April 1999).

Similar requirements have also been described by the Ontario Court of Appeal in a case involving a request for access to records of tribunal hearings containing a requester's personal information prepared by a private freelance court reporter: (Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner) [1999] O.J. No. 4072). The Court said:

> It is reasonable to expect that the Board would ensure, by contract if necessary, that any records … be used solely for the purposes of the Board. The Board can and should exercise control over the use of all records made by court reporters of its proceedings.
>
> The Board chose to enter into arrangements with independent court reporters to meet its court reporting requirements.... The Board's failure to enter into a contractual arrangement with the reporter that would enable it to fulfil its statutory duty to provide access to documents under its control cannot be a reason for finding that the duty does not exist. Put another way, the Board cannot avoid the access provisions of the Act by entering into arrangements under which third parties hold custody of the Board's records that would otherwise be subject to the provisions of the Act.

In the same case, the Divisional Court made the following comments regarding the institution's obligations to enter into appropriate contractual arrangements:

> The Inquiry Officer and this court are entitled to assume that the Board's contractual arrangements with the reporter are appropriate to ensure compliance with its statutory obligations.
>
> ...
>
> If in fact its contract with the reporter is inadequate to ensure that the Board is in compliance with its statutory duties under [the *Act*], it is not obvious to me that this would provide a basis to refuse an otherwise valid access to information request ... The Board is not entitled to "contract out" of its statutory obligations."

Although the court's decisions dealt with the individual right of access provisions of the *Act*, the same principles require institutions to ensure compliance with the privacy provisions of the *Act* where a third party contractor is engaged to perform functions on behalf of government involving the disclosure of personal information to the contractor.

With these principles in mind, we make the following observations regarding the general and survey specific measures to which the Ministry has referred us.

(1) The prohibition against release of POSO customer account information to anyone other than account holders, their authorized representatives, or as required by law, as set out in POSO's Operational Procedures Manual, was not respected. This is demonstrated by our findings on the Ministry's non-compliance with section 42 of the *Act*.

(2) The June 1995 Information and Privacy Bulletin attaching "Suggested Terms for Use in Contracts Dealing with the Disclosure of Personal Information" was, in its own words, designed to ensure that "confidentiality clauses are included in all consulting contracts in which the consultant will have access to confidential and/or personal information." The "Suggested Terms" document makes clear reference to the various personal privacy protection requirements of the *Act*. However, the bulk of the suggested protections set out in this document, including those relating to confidentiality, records management, security, use and disclosure, retention and disposal of personal information, among others, were **not** incorporated into either of the consulting contracts between Privatization and Angus Reid or Privatization and Wood Gundy.

(3) The Angus Reid and Wood Gundy contracts contain and/or incorporate by reference from "Standing Agreements" or "Standing Guidelines" (but from not the 1995 "Suggested Terms" document) confidentiality provisions of the most general sort, requiring that:

    (i) confidential information only be used for the purposes of performing the particular assignment;

    (ii) the information remains the property of the government during and following the assignment; and

    (iii) the information shall not be disclosed to any third party without the government's specific written consent.

In light of the language and context within the contracts, these provisions are clearly designed to protect the financial, competitive and intellectual property interests of government, and are not designed to protect the personal privacy interests of POSO customers. We note that the care taken to protect government's commercially valuable information was not taken to protect the personal information of POSO customers.

(4) The only reference to the *Act* in either of these contracts is to the effect that information provided by the consultants to the government are subject to the provisions of the *Act*. Contract clauses of this nature are designed to put bidders and contractors on notice that their commercial information provided to government may be subject to the general right of access provisions of the *Act*. These clauses make no reference whatsoever to the privacy protection provisions of the *Act*. More specifically, the Angus Reid Standing Agreement does **not** recite, as the Ministry submits, "that the Standing Agreement is governed by the *Act*." Rather, it states that the agreement is "subject to" the *Act*, a reference to the fact that the agreement itself may be disclosed pursuant to an access request under the *Act*.

(5) The July 29, 1997 assurances from Angus Reid to Privatization were given after the disclosure to Angus Reid. These assurance do not have the force of law or contract behind them, and are an inadequate substitute for clear contractual protections in light of the detailed requirements of the *Act* in the collection, retention, use, disclosure, security and destruction of personal information. The Ministry's own 1995 "Suggested Terms" document would have served as a starting point for the necessary contractual protections.

(6) The July 28 and July 31, 1997 verbal assurances of compliance with the *Act*, apparently given by the Ministry's Freedom of Information Co-ordinator, were in error. The disclosures were clearly **not** in compliance with the *Act*. We have been unable to confirm the existence or nature of any legal advice on which the Co-ordinator's assurances were apparently based. Moreover, as we have previously noted, any assurances were only sought and received in relation to the disclosure to Angus Reid, not the disclosure to Wood Gundy, and even then only after the disclosure had already taken place. Further, on July 28, 1997, the Ministry Co-ordinator also advised Privatization that it had disclosed more personal information to Angus Reid than was necessary for the survey, and that he was unable to comment on the adequacy of the confidentiality clause in the Angus Reid agreement because he had not seen it. Privatization then faxed a copy of the contract to the Co-ordinator, who reviewed it . On July 28 or 29, 1997, the Ministry's Co-ordinator had a conversation with Privatization about the adequacy of the confidentiality provisions and advised Privatization that the provisions needed strengthening.

(7) The April 28, 1997 letter from OFA's CEO, which was made available to account holders upon request, has no bearing on the security and confidentiality of their personal information.

(8) The Ministry has provided no submissions on the security and confidentiality of the personal information disclosed to Wood Gundy.

(9) Except for the contractual clauses and "assurances" to which the Ministry referred us, we have no additional information on the security and confidentiality of the information provided to Privatization. Most notably, we have no information whatsoever on the use of the printout of account holders' personal information provided to Privatization.

M121

IMPORTANT NOTE CONCERNING THE FOLLOWING PAGES

THE PAGES WHICH FOLLOW HAVE BEEN FILMED TWICE IN ORDER TO OBTAIN THE BEST REPRODUCTIVE QUALITY

USERS SHOULD CONSULT ALL THE PAGES REPRODUCED ON THE FICHE IN ORDER TO OBTAIN A COMPLETE READING OF THE TEXT.

REMARQUE IMPORTANTE CONCERNANT LES PAGES QUI SUIVENT

LES PAGES SUIVANTES ONT ÉTÉ REPRODUITES EN DOUBLE AFIN D'AMÉLIORER LA QUALITÉ DE REPRODUCTION

LES UTILISATEURS DOIVENT CONSULTER TOUTES LES PAGES REPRODUITES SUR LA FICHE AFIN D'OBTENIR LA LECTURE DU TEXTE INTÉGRAL

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

In our view, any contract with a consultant involving the transfer of personal information should contain provisions which explicitly provide that the *Act* applies to records in the hands of the third parties. The contract should:

- specify the types or classes of records to be transferred or generated in the provision of the service;
- acknowledge that the records continue to remain under the institution's control; and
- oblige third parties to keep the records secure and return them to the institution on demand for the purposes of an access request, or in the event that a privacy issue arises.

The contract should also require that the records, together with any copies or extracts, be returned to the institution at the conclusion of the contract, to ensure that continuing rights of access and privacy are not frustrated.

Most importantly, it should be clearly stated that privacy rules governing the collection, retention, use, disclosure and security of personal information continue to apply while the agreement is in effect and thereafter. In particular, the contract should specify that, except as may be permitted by the *Act*:

- only employees of the consultant who require the personal information in the course of performing their duties should be permitted access to it;
- the information cannot be used by the consultant for its own purposes or, for any other purpose not identified in the contract;
- the information cannot be disclosed or transferred to other third parties without the informed consent of the individuals concerned; and
- the consultant must take all necessary measures to provide individuals with the right of access to their own personal information, in accordance with the requirements of the *Act*.

This list is by no means exhaustive. The "Model Agreement" and "Best Practices" papers produced by our Office more fully describe the types of protections which should be set out in clear and detailed contractual language. The "Safeguards for Personal Information" and "Recommendations" portions of Investigation Report I97-017P also provide further guidance in this respect.

The Ministry did not take reasonable steps with respect to the security and recovery of the information disclosed to Privatization, Angus Reid and Wood Gundy. We are satisfied, however, that the information was, in fact, treated securely in the hands of Angus Reid and Wood Gundy, and that the bulk of the information was either fully recovered by POSO and the government auditor or destroyed or anonymized by Angus Reid and Wood Gundy. Without any information directly from Privatization, we are not satisfied that the personal information provided to it in the form of either the CD-ROMs or the printout of account holder information was handled securely.

Conclusion: **Reasonable measures were not taken with respect to the security of the information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*.**

In our view, any contract with a consultant involving the transfer of personal information should contain provisions which explicitly provide that the *Act* applies to records in the hands of the third parties. The contract should:

- specify the types or classes of records to be transferred or generated in the provision of the service;
- acknowledge that the records continue to remain under the institution's control; and
- oblige third parties to keep the records secure and return them to the institution on demand for the purposes of an access request, or in the event that a privacy issue arises.

The contract should also require that the records, together with any copies or extracts, be returned to the institution at the conclusion of the contract, to ensure that continuing rights of access and privacy are not frustrated.

Most importantly, it should be clearly stated that privacy rules governing the collection, retention, use, disclosure and security of personal information continue to apply while the agreement is in effect and thereafter. In particular, the contract should specify that, except as may be permitted by the *Act*:

- only employees of the consultant who require the personal information in the course of performing their duties should be permitted access to it;
- the information cannot be used by the consultant for its own purposes or, for any other purpose not identified in the contract;
- the information cannot be disclosed or transferred to other third parties without the informed consent of the individuals concerned; and
- the consultant must take all necessary measures to provide individuals with the right of access to their own personal information, in accordance with the requirements of the *Act*.

This list is by no means exhaustive. The "Model Agreement" and "Best Practices" papers produced by our Office more fully describe the types of protections which should be set out in clear and detailed contractual language. The "Safeguards for Personal Information" and "Recommendations" portions of Investigation Report I97-017P also provide further guidance in this respect.

The Ministry did not take reasonable steps with respect to the security and recovery of the information disclosed to Privatization, Angus Reid and Wood Gundy. We are satisfied, however, that the information was, in fact, treated securely in the hands of Angus Reid and Wood Gundy, and that the bulk of the information was either fully recovered by POSO and the government auditor or destroyed or anonymized by Angus Reid and Wood Gundy. Without any information directly from Privatization, we are not satisfied that the personal information provided to it in the form of either the CD-ROMs or the printout of account holder information was handled securely.

Conclusion: Reasonable measures were not taken with respect to the security of the information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*.

SUMMARY OF CONCLUSIONS

In summary, we conclude that:

(A) The information in question was "personal information" as defined in section 2(1) of the *Act*.

(B) The three disclosures of personal information, (a) from POSO to Privatization, (b) from Privatization to Angus Reid, and (c) from POSO to Wood Gundy, were not in compliance with the *Act*.

(C) Reasonable measures were not taken with respect to the security of the information and its recovery from Privatization, Angus Reid, and Wood Gundy, in accordance with the requirements of section 4 of Regulation 460 of the *Act*.

Remedial Steps taken by the Ministry

In response to the 1997 incident, the Ministry advises that it has taken the following remedial steps:

(1) A new sign-off procedure was announced in a memo dated August 22, 1997 from the Chief Executive Officer (CEO) of the OFA to all OFA staff whereby no disclosure of personal information and no new use of personal information can be made without first obtaining the approval of the CEO of the OFA or in that person's absence, legal counsel.

(2) The CEO's memo dated August 22, 1997 also reminds OFA staff that personal information should not be distributed or shared within the organization except where there is a need for the recipient to receive the information in order to perform his or her job.

(3) Training sessions were conducted by legal counsel from Management Board Secretariat in late August and early September 1997. These sessions emphasized privacy protection and were attended by senior staff at the Privatization Secretariat and by the POSO Freedom of Information and Privacy Liaison Officer.

(4) The Ministry submits that it has a network of Freedom of Information and Privacy Liaison Officers throughout the Ministry, including POSO. The Ministry's Freedom of Information and Protection of Privacy Office provides ongoing training and monthly bulletins on access and privacy issues to all Freedom of Information and Privacy Liaison Officers and sometimes, depending on their contents, to senior executives.

(5) The Ministry requires that any known breaches of the *Act* be reported to the CEO of the OFA and OFA's Board of Directors through the OFA's legal counsel as part of the general legal compliance report given at each quarterly Board meeting.

(6) The POSO Operational Procedures Manual used by staff was recently revised to fully deal with the requirements of the *Act*. These revisions were distributed to all POSO Managers whereby they were instructed to ensure that all staff were made aware of the importance of these materials.

(7) Staff at POSO are addressing the requirements relating to personal information banks maintained by the organization to update the index of these banks and ensure that records of use and other notices relating to personal information are issued and updated as appropriate, including the 1997 POSO privatization review.

(8) Precedent contract clauses dealing explicitly with the *Act* were provided for inclusion in POSO's contracts with third parties that collect or use personal information.

We note that some of these steps were not implemented until after our Office began investigating this matter, despite that fact that this incident happened almost three years ago. For example, the revision to the operational procedures manual is dated February 25, 2000, after the date we began this investigation. Updates to the personal information banks, records of use, and notice of purpose of collection were only approved in March 2000, two months after this investigation commenced.

We also note that some of these procedures appear to have existed prior to the 1997 disclosure and thus are not new. For example, while the network of Freedom of Information and Privacy Liaison Officers appears to have been expanded, the POSO Liaison Officer has existed (at least) since September 1995 [since the Liaison Officer's name appears on a September 1995 list].

While quite beneficial by comparison, we find these remedial steps to be inadequate in preventing future disclosures of personal information. Our comments on how to improve on these steps are contained in the recommendation section of this report.

Final Comments

We reviewed the 1997 incident involving POSO because we felt that the public had not been given assurances that its personal information had been returned to government. Since we have no evidence that POSO had advised its customers of the potential for these disclosures, we can only conclude that most individuals would not have known about or expected such a disclosure until recently. We believe that the Ministry had a responsibility to notify individuals whose personal information was at issue at the time the disclosures took place. By not informing them at the time, individuals were not able to make informed choices and exercise their rights under the *Act*. Had they known about the incident earlier, they may have brought it to our attention. Had we known about it earlier, we may have been able to confirm and report on these events with greater accuracy. The passage of time has clearly made this task more difficult.

Many unanswered questions remain. What we do know is that the outcome could have been much worse if Angus Reid and Wood Gundy had not taken the care they did to ensure that the personal information in their possession was not more widely circulated.

It is critical that the government put into place the proper checks and balances to ensure that any personal information released to external sources does not contravene the protections found in the *Act*. The government must scrutinize each initiative to ensure that protecting privacy is a component of each workplan. Our Office has always recommended that privacy be "built in" upfront, and addressed at the planning stage. Failing to do so invariably leads to problems down the road, resulting in far more time being spent on correcting those problems than in addressing them initially.

Personal financial information is a particularly sensitive privacy concern in light of its potential for use or misuse, for a variety of purposes such as profiling, marketing, surveillance and even securing unauthorized access to individual accounts. Intrusions in the area of personal financial affairs are thus deserving of the utmost protection afforded by privacy legislation. This protection includes the provision of adequate notice of uses or disclosures of financial information for reasons other than those for which it collected or, failing that, the individual's informed consent for a specific use or disclosure.

At a minimum, Fair Information Practices require that individuals be given the choice of opting "in" or opting "out" of the use or disclosure of their financial information for secondary purposes such as personal profiling or marketing surveys. In many cases, such consent will be forthcoming where, as in this case, POSO account holders may well have an interest in letting their views on privatization be known to the government. On the other hand, some individuals may not want to be questioned about such issues in an intrusive fashion by persons unknown, acting on the government's initiative, and having knowledge of their financial affairs. When such activity is engaged in by government, it is ultimately coercive and clearly becomes a proper matter for privacy laws to govern, and for privacy oversight bodies to address, in those cases where privacy rights are not respected.

Attention to the protection of these rights is required on an urgent and focused basis, as many domestic and global initiatives demonstrate. The *Personal Information Protection and Electronic Documents Act* (Bill C-6), a federal government statute extending privacy protections to the private sector, is one such initiative made law this spring, to come into force January 1, 2001. Where such laws presently exist to govern the public sector in this province, our Office would be remiss if we did not take immediate and decisive steps to investigate and report on complaints and allegations of privacy infringements of this nature. While we would not describe the events of 1997 as a worst-case scenario, this incident is evidence that much work remains to be done. As always, our Office is prepared to work with the Ministry and other branches of government to ensure that the necessary protections are addressed and implemented on all fronts. In the end, privacy can only be protected in a comprehensive manner through the co-operation and concerted efforts of all those involved.

RECOMMENDATIONS

Recommendations to the Ministry of Finance:

(1) The new executive sign-off procedure at the Ontario Financing Authority (OFA) should explicitly incorporate legal advice as part of the approvals process where the use or disclosure of personal information is implicated.

(2) Freedom of Information and Privacy training sessions should: (a) be expanded to OFA staff who handle personal information as part of their regular duties; (b) explain circumstances which may not be in compliance with the *Act* for both internal and external disclosures; (c) review case scenarios; and (d) when in doubt, advise whom to consult.

(3) Freedom of Information and Privacy training should be mandatory for personnel engaged in privatization or alternative service delivery initiatives and be incorporated into staff training and/or orientation. It is important that staff be made aware of privacy issues, the need for executive sign-offs, as well as legal input, *prior* to any disclosure.

(4) The Operational Procedures Manual used by staff involved in privatization initiatives should be revised to deal fully with the requirements of the *Act*.

(5) The Ministry should immediately attach or link to all POSO account holders' personal information, a record of the 1997 disclosure to Angus Reid and CIBC Wood Gundy, pursuant to section 46(1)(b) of the *Act*. This was referenced in the material sent to us by the Ministry, but it is not clear whether this has been done.

(6) POSO customers should be provided with an individualized notice of collection (required by section 39(2) of the *Act*) at the time of the collection of personal information, i.e., when they first open an account. Notices should be incorporated into the bank forms used to collect the personal information, as appropriate. If original notices are revised, they should be provided to customers on an individual basis, i.e., mailed to them directly.

(7) The Ministry should review and revise its contracts to ensure consistency with the observations made on page 23 on the types of clauses that should be included in consulting agreements to enhance compliance with the *Act*. The Ministry should provide us with a copy of its review.

Within six months of receiving this report, the Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with these recommendations.

Recommendations to the Government of Ontario:

(1) Upon learning of a possible incidence of non-compliance with the *Freedom of Information and Protection of Privacy Act*, a government organization should notify the Commissioner as quickly as possible.

(2) The government should carefully scrutinize each initiative to ensure that privacy protection is a key component of every workplan including any technological requirements. The design of government information systems should be sufficiently flexible to facilitate the extraction and separation of personal identifiers from the remainder of a database. Computer systems should be designed with privacy in mind.

(3) In April 1999, our Office published a paper entitled, *Best Practices for Protecting Personal Privacy in Conducting Survey Research* (Appendix D). This paper was developed in collaboration with the Ministry of Labour and the Corporate Freedom of Information and Privacy Office of Management Board Secretariat. We recommend that all institutions review this document prior to conducting any survey research.

April 26, 2000

Ann Cavoukian, Ph.D.
Commissioner

Date

***

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

ADDENDUM

TO A SPECIAL REPORT TO
THE LEGISLATIVE ASSEMBLY OF ONTARIO
ON THE DISCLOSURE OF PERSONAL INFORMATION
BY THE PROVINCE OF ONTARIO SAVINGS OFFICE,
MINISTRY OF FINANCE

POWERS NECESSARY TO CONDUCT A PROPER INVESTIGATION

April 26, 2000

Submitted by
Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

Obstacles We Encountered During this Investigation

This investigation clearly demonstrates the need for explicit statutory powers to enable the Information and Privacy Commissioner to conduct a full and complete investigation.

As referenced in the investigation report, we were unable to conduct a full and complete investigation in this case for a number of reasons, which are outlined below:

1. During the period from January 13 through January 31, 2000, the Ministry of Finance engaged our Office in a series of protracted discussions designed, in our view, to restrict the scope of our investigation and the investigative tools available to us, as specified below.

2. We were asked to conduct primarily a paper-based review of the events that had transpired, and only to conduct interviews if necessary, to clarify any ambiguities or uncertainties. We were also asked to provide interviewees with the written questions we intended to use, in advance of the interviews to be conducted. We did not agree to these terms.

3. On January 25, 2000 we received a letter from the Deputy Minister of Finance which began by questioning our authority to conduct this investigation. It then set out a number of restrictions and parameters for the investigation. For example, the letter stated:

   > "I assume that at this stage, you will not be contacting any individuals other than myself as part of your investigation. If you do intend to do so, I expect that you would notify me in advance so that I can address any resulting issues."

4. We were not given any reason for the government's reticence in this particular case, unlike other cases. This was the source of some concern, given our past experience in similar matters where full co-operation had been immediately forthcoming. We did not agree to restrict our ability to investigate.

5. In early February, after further discussions regarding our authority to investigate and renewed assurances of full co-operation, we asked the Ministry to contact certain employees, current and former, who had knowledge of relevant events, to ask them to give us their full and complete co-operation during the investigation. While the Ministry's letter to employees referred to its own co-operation, it added "*...you are free to make your own decision as to how to respond to the Commission's request to question you during this investigation*." We had urged the Ministry instead to use language that was designed to encourage employees to co-operate with us. We were told by one individual's lawyer that his client had initially been willing to talk to us but was reluctant to do so after having received the Ministry's letter.

6. As a consequence of these delays, our first interview did not take place until February 14, well beyond the date by which the Commissioner had hoped to *complete* the initial part of her investigation and issue a report (January 31), and had stated so publicly.

7. It is interesting to note that all the private sector organizations involved in this matter co-operated with us fully and immediately. In contrast, a number of senior ranking government employees and former employees, identified as the key players, either refused to be interviewed, ignored our request outright, or were only willing to be interviewed on conditions unacceptable to the Commissioner (e.g., only agreeing to respond in writing to written questions provided to them, requesting assurances of complete anonymity, etc.). We feel these individuals should have owed a continuing duty to their present or former government employer to co-operate with the Commissioner's investigation by explaining their official roles in a matter of public importance such as this.

8. Some documents sent to us were partially blacked out or "severed," even though the Ministry is well aware of the fact that we routinely review highly sensitive *unsevered* documents and are bound by a statutory duty of confidence. Not only was this highly out of the ordinary, but in our view, disrespectful of the mandate of this Office.

The Ministry submitted that it has been "frank and open" and has "...made every effort to assist you with your review." We respectfully disagree. For example, the Commissioner called the Deputy Minister on February 11, 2000, to specifically advise him that no one from the Ministry or the Privatization Secretariat had agreed to be interviewed to date, and that this would be reflected in the investigation report. While the offer of co-operation was again reiterated, no one from Privatization came forward and agreed to be interviewed. It was only after the Ministry received our draft report on March 31, 2000 that we were offered further assistance in answering any unanswered questions. Given our experience in dealing with the Ministry throughout this investigation, we believed that the offer to provide assistance, at such a late stage in the process, would not prove to be fruitful and would only further delay the release of the final report.

The Ministry's efforts to limit our investigation and its failure, in our view, to use its best efforts to ensure that its current and former employees co-operated with us has hindered this investigation. Much of our fact-finding has, of necessity, been restricted to a review of documents provided by the Ministry, supplemented by information obtained through interviews with those individuals who agreed to meet with us.

As a consequence, the following issues have been left unexamined or unresolved:

1. We still do not have a complete picture of the activities of POSO and, in particular, the decision-making processes, that led to the disclosure of the personal information in question, namely, the account holder information.

2. We are unable to provide any meaningful comment on the role played by the Privatization Secretariat in these events, since none of Privatization's former employees were willing to be interviewed by us during the course of this investigation.

3. We have no first-hand knowledge of any deliberations within the Privatization Secretariat about the advisability of disclosing the account holder information to the private sector. For example, we cannot report on:

(i) what privacy considerations, if any, were contemplated in handling this information;

(ii) what privacy protocols, if any, were in place for conducting privatization reviews;

(iii) what approvals were sought and received by Privatization for disclosing the information in question, as POSO claimed had occurred;

(iv) what legal advice, if any, was sought and received by Privatization in respect of the disclosures;

(v) whether Privatization staff were aware that they were bound to comply with the privacy protections in the *Act*;

(vi) whether Privatization staff had received any training on the requirements of the *Act*;

(vii) whether Privatization staff had actually accessed, reviewed or otherwise used the information for any purpose.

4. According to Ministry records, POSO had sent Privatization a printout of client account information from five branches on August 5, 1997 (a complete description is set out in the investigation report), which was returned to POSO on or about August 21, 1997. We do not have any information as to why this report was generated for Privatization, what it was used for, who saw it, or whether any copies of it were made.

5. In approaching this investigation, we identified a preliminary list of those persons who appeared to be directly involved in the events of 1997, with the most responsibility and the greatest amount of information to offer. The Ministry was provided with this list and was asked for its assistance in arranging the interviews. Since a number of these persons ultimately could not be interviewed, we are not satisfied that all *other* individuals with pertinent knowledge to impart have indeed been identified.

6. We do not have the complete facts regarding the 1995 POSO survey. For example, were there account holder complaints arising from that survey?

As a consequence, we are not completely satisfied as to the source or nature of the systemic deficiencies that existed in 1997: whether these lay primarily with Privatization, or POSO, or both. Because some of our conclusions are based on assumptions and hearsay rather than on direct, first-hand evidence, we have been constrained in making meaningful recommendations to ensure that similar disclosures do not occur in the future, and to provide appropriate guidance to other government institutions.

The Ministry's response to our investigation stands in stark contrast to the co-operation provided to the government auditor who conducted the review (not privacy audit) of these events in August of 1997. The auditor advised us that he had been asked on August 21, 1997 to conduct his review and to report back by August 25, which he did. According to the auditor, Ministry employees had been clearly instructed to co-operate with him. Our Office, however, was told by Ministry officials that they were not in a position to instruct their employees to co-operate with us, not even to the point of encouraging them to participate in the interview process.

The Ministry's response was also in contrast to the actions taken by the Ministry of Health during an investigation undertaken by our Office in 1996. In that case, the Minister of Health had stepped aside pending an investigation into an incident involving one of his assistants. Our Office was asked to conduct an investigation by the Secretary of Cabinet on December 9, 1996, as promptly as possible. Within 10 days, we were able to interview seven of the key individuals. We completed the remaining 11 interviews within approximately five weeks, which encompassed a two- week period over the Christmas holidays, when no interviews took place. Not one person from the government refused to be interviewed by our Office, and we received, what can accurately be described as, "full and complete co-operation." Our report was released on February 20, 1997, roughly two and a half months after the incident took place.

Despite our inquiries, we have been offered no explanation for these dramatically different approaches. As a consequence, we do not feel that the public interest has been adequately served.

Our experience with this investigation has clearly pointed to the deficiencies in the legislative powers and authority provided to the Commissioner in discharging her responsibility to conduct privacy investigations.

Absence of Powers and Authority to Investigate

Section 58 of the *Act* requires the Commissioner to make an Annual Report to the Legislature. This report must contain "a comprehensive review of the effectiveness of the *Act* ... in providing ... protection of personal privacy, including ... an assessment of the extent to which institutions are complying with this *Act* ... and the Commissioner's recommendations with respect to the practices of particular institutions."

It is not possible to perform the comprehensive review, assessment and recommendation duties mandated by section 58 without the ability to gather the information necessary to discharge these responsibilities.

Specifically in the context of our privacy protection responsibilities, we cannot adequately assess the extent to which institutions are complying with the collection, retention, use and disclosure provisions in Part III of the *Act* unless we are able to gather all pertinent information from institutions and members of the public in the course of investigating specific complaints.

Unlike virtually every other privacy statute we are aware of, Ontario's *Act* does not include a detailed statutory framework for dealing with privacy complaints. (Such regimes now exist in British Columbia, Alberta, Saskatchewan, Manitoba, Quebec, the Yukon, and under federal privacy legislation.) Although the Commissioner has the responsibility to respond to complaints and conduct investigations, she must do so without the power to summons and examine individuals under oath, or to compel the production of documents relevant to the investigation. In other words, we are completely dependent on the co-operation and goodwill of the government and individual witnesses.

We are also faced with the additional concern, frequently expressed by individuals whom we wish to interview, that the *Act* makes no provision for protecting them from civil, criminal or quasi-criminal liability arising out of statements made to the Commissioner's staff in the course of our interviews and investigations. Under the statutory privacy regimes of other provinces and the federal government, statements made by witnesses in the course of investigations cannot be used to form the basis of libel or slander actions against them because their statements are considered to be "privileged" under those regimes. Similarly, while witnesses cannot refuse to answer questions on the grounds that their statements might incriminate them, or establish their liability in a civil proceeding, their statements cannot be used as evidence against them in any court or other proceedings except on a trial for perjury. Such protections are presently afforded to individuals who make statements to the Commissioner in the course of her inquiries into access appeals under section 52 of the *Act*; however, they are not currently afforded to individuals who make statements in the course of the Commissioner's privacy investigations. The reluctance of many individuals to speak with us in this investigation is directly attributable to the lack of witness statement protections which would be available under an investigation regime with formal processes.

We have operated under the current scheme since the *Act* first came into force, in 1988. In routine, non-controversial cases, our investigations have, for the most part, been undertaken by way of an exchange of correspondence with the particular institution involved. Interviews and documentary reviews have formed an essential component of a number of other investigations involving more controversial or high profile incidents, with a significant degree of public interest. Co-operation has been difficult to obtain on occasion, but we have never before faced the level of difficulty or the number of obstacles experienced in this investigation.

It is abundantly clear that the present situation should not continue. We are confident in saying that the public expects its Privacy Commissioner to decide what type and what level of investigation is required in a particular situation, and to have the power and authority to ensure that all investigations are thorough and complete. Unless the *Act* is amended to provide explicit powers in this area, the particular government institution involved in a potential privacy incident will be the one to decide whether and to what degree the incident warrants investigation. We can attempt to investigate, but without the coercive powers normally associated with an investigative mandate, such as the authority to order the production of records, to enter and inspect premises, and to summons and examine witnesses under oath, we will always be dependent on the co-operation of the particular government institution. Similarly, we will continue to be hampered by the absence of the various witness protections provided by other statutory regimes.

The experience of this particular investigation clearly demonstrates why the system needs to be amended and why these coercive powers are required. Without the appropriate powers, individuals with relevant information can and will, on occasion, refuse to co-operate.

It should also be noted that this is not the first time we have asked for statutory amendments in this area. In 1991 and 1994, we made submissions to the Standing Committee on the Legislative Assembly during its three-year reviews of the provincial and municipal *Acts*. In both instances we recommended, among other things, that the *Acts* be amended to give the Commissioner express power and authority to conduct investigations and to enter premises to inspect records for this purpose. On both occasions the Standing Committee agreed with our suggestions and recommended in favour of amendments of this nature so that the Commissioner could "efficiently and effectively perform the mandate of the legislation." Unfortunately, these much-needed amendments were never brought forward.

The absence of explicit powers has prevented us from conducting a thorough investigation in this case. As a result, we had no choice but to investigate as best we could and to report on our findings. This we have done, but we are not satisfied with the experience or the results of this investigation. We do not think the government should be satisfied either. All of the questions surrounding the 1997 disclosure of POSO account holder information have not been answered, nor have all of the relevant facts been determined. This is unacceptable to us. It should be unacceptable to the government.

Recommendation to the Government of Ontario

We call upon the government, in the strongest terms possible, to introduce amendments to the *Act*, providing Ontario's Commissioner with the same type of clear and explicit powers and authority to conduct privacy investigations that are available to other Privacy Commissioners in Canada, and to do so by the end of this legislative term. We feel that the existing inquiry system for access to information appeals under Part IV of the *Act* is a comprehensive and readily adaptable model for the introduction of a formal privacy investigation regime in Ontario. We have attached Appendix E to this Report which contains our recommended changes to Part IV of the Act, and we would be pleased to work with the government in this regard and offer whatever assistance may be required.

Ann Cavoukian, Ph.D.
Commissioner

April 26, 2000
Date

***

APPENDICES

A List of Individuals with Whom Interviews Were Requested and Individuals Interviewed

B *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, s. 42, s. 52

C A Model Access and Privacy Agreement, IPC, August 1997

D Best Practices for Protecting Individual Privacy in Conducting Survey Research (Full Version), IPC, April 1999

E IPC's proposed amendments to the *Freedom of Information and Protection of Privacy Act* to provide for explicit powers and processes in relation to the investigation of complaints and review of compliance with Part III of the *Act* (Protection of Individual Privacy)

APPENDIX A

LIST OF INDIVIDUALS WITH WHOM INTERVIEWS WERE REQUESTED:

Ministry of Finance

Ontario Financing Authority
Tony Salerno, Vice Chair & CEO

Province of Ontario Savings Office
David Brand, Director
Alan Parsons, Manager

Freedom of Information and Protection of Privacy Office
Fred Jones, Freedom Of Information Co-ordinator

Privatization Secretariat

Paul Currie, CEO
Phil Symmonds, Vice President
James Small, Project Officer
Marilyn Hood*, Communications Director

Management Board Secretariat

Peter Alexander, Manager, Operational Audit

Angus Reid Group

Martin Redfern, Research Manager

CIBC Wood Gundy

David Leith, Managing Director
Catherine Code, Associate Director
Patrice Ouimet, Analyst
Shane Szeto**, Summer Student

* Could not be located
** No longer with CIBC Wood Gundy

N.B. Titles noted above date back to 1997

INDIVIDUALS INTERVIEWED:

Ministry of Finance

Ontario Financing Authority
No one

Province of Ontario Savings Office
David Brand
Alan Parsons (telephone interview)

Freedom of Information and Protection of Privacy Office
Fred Jones

Privatization Secretariat

No one*

Management Board Secretariat

Peter Alexander

Angus Reid Group

Martin Redfern

CIBC Wood Gundy

James McSherry
David Leith
Catherine Code
Patrice Ouimet (telephone interview)
Shane Szeto** (telephone interview)

---

* While James Small did finally agree to an oral interview, it was only after protracted negotiations regarding the conditions of the interview, and at a point where we had already completed our investigation and issued the draft report.

** No longer with CIBC Wood Gundy

APPENDIX B

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F-31, sections 42 and 52

42. An institution shall not disclose personal information in its custody or under its control except,

(a) in accordance with Part II;

(b) where the person to whom the information relates has identified that information in particular and consented to its disclosure;

(c) for the purpose for which it was obtained or compiled or for a consistent purpose;

(d) where disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions;

(e) for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement thereunder;

(f) where disclosure is by a law enforcement institution,

  (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or

  (ii) to another law enforcement agency in Canada;

(g) where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

(h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

(i) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

(j) to a member of the Legislative Assembly who has been authorized by a constituent to whom the information relates to make an inquiry on the constituent's behalf or, where the constituent is incapacitated, has been authorized by the next of kin or legal representative of the constituent;

(k) to a member of the bargaining agent who has been authorized by an employee to whom the information relates to make an inquiry on the employee's behalf or, where the employee is incapacitated, has been authorized by the next-of-kin or legal representative of the employee;

(l) to the responsible minister;

(m) to the Information and Privacy Commissioner; and

(n) to the Government of Canada in order to facilitate the auditing of shared cost programs.

52. (1) The Commissioner may conduct an inquiry to review the head's decision if,

(a) the Commissioner has not authorized a mediator to conduct an investigation under section 51; or

(b) the Commissioner has authorized a mediator to conduct an investigation under section 51 but no settlement has been effected.

(2) The *Statutory Powers Procedure Act* does not apply to an inquiry under subsection (1).

(3) The inquiry may be conducted in private.

(4) In an inquiry, the Commissioner may require to be produced to the Commissioner and may examine any record that is in the custody or under the control of an institution, despite Parts II and III of this Act or any other Act or privilege, and may enter and inspect any premises occupied by an institution for the purposes of the investigation.

(5) The Commissioner shall not retain any information obtained from a record under subsection (4).

(6) Despite subsection (4), a head may require that the examination of a record by the Commissioner be of the original at its site.

(7) Before entering any premises under subsection (4), the Commissioner shall notify the head of the institution occupying the premises of his or her purpose.

(8) The Commissioner may summon and examine on oath any person who, in the Commissioner's opinion, may have information relating to the inquiry, and for that purpose the Commissioner may administer an oath.

(9) Anything said or any information supplied or any document or thing produced by a person in the course of an inquiry by the Commissioner under this Act is privileged in the same manner as if the inquiry were a proceeding in a court.

(10) Except on the trial of a person for perjury in respect of his or her sworn testimony, no statement made or answer given by that or any other person in the course of an inquiry by the Commissioner is admissible in evidence in any court or at any inquiry or in any other proceedings, and no evidence in respect of proceedings before the Commissioner shall be given against any person.

(11) A person giving a statement or answer in the course of an inquiry before the Commissioner shall be informed by the Commissioner of his or her right to object to answer any question under section 5 of the *Canada Evidence Act*.

(12) No person is liable to prosecution for an offence against any Act, other than this Act, by reason of his or her compliance with a requirement of the Commissioner under this section.

(13) The person who requested access to the record, the head of the institution concerned and any affected party shall be given an opportunity to make representations to the Commissioner, but no person is entitled to be present during, to have access to or to comment on representations made to the Commissioner by any other person.

(14) The person who requested access to the record, the head of the institution concerned and any affected party may be represented by counsel or an agent.

APPENDIX C

Model Access and Privacy Agreement

Information
and Privacy
Commissioner/
Ontario

Model Access and Privacy Agreement

Ann Cavoukian, Ph.D.
Commissioner

August, 1997

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of *John Eichmanis* in preparing this report.

This publication is also available on the IPC Web site. Upon request, this publication will be made available on audio tape.

Table of Contents

Introduction 1
Considerations for Alternative Service Delivery Contracts or Agreements 1
Transitional Provisions Included in the Agreement 1
1. Custody or control of general records and personal information 1
2. Physical transfer of general records and personal information 2
3. Outstanding Requests and Appeals 2

Model Access and Privacy Agreement 2
I. Purpose 3
II. Definitions 3
III. Policies 4
1. Accountability and Administration 4
2. Protection of Personal Information 5
Collection 5
Individual Access 5
Use and Disclosure 5
Consent 6
Retention 6
Disposal 6
Accuracy 6
Right of Correction 6
Security 7
Complaints 7
Penalties 7
3. Access to Information 7

Introduction

To assist government organizations when contemplating alternative service delivery options, the Office of the Information and Privacy Commissioner/Ontario (the IPC) has prepared a model agreement that could form part of the overall contract or agreement between the government organization and the contracting entity. The model agreement or contract would be appropriate in those circumstances where the government organization does not retain custody or control of its general records or personal information.

While the suggested provisions seek to be inclusive, the specific circumstances of each agreement or contract may require modifications to some provisions.

Considerations for Alternative Service Delivery Contracts or Agreements

The agreement or contract should contain:

1. transitional provisions; and
2. access and privacy provisions attached as a schedule to the agreement or contract (see "Model Access and Privacy Agreement").

Transitional Provisions Included in the Agreement

1. Custody or control of general records and personal information

The agreement or contract should include reference to whether the government organization will retain custody or control of the general records and personal information in its possession.

The government organization should consider whether it will transfer custody or control of the general records or personal information to the contracting entity, or whether it will retain custody or control, while transferring certain responsibilities for the general records and personal information to the contracting entity. By determining who has custody or control of the records, the government organization is able to decide whether the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts)* will continue to apply. For example, if the government organization retains custody or control, the *Acts* will still apply to the records. However, if custody or control is to be passed to the Alternative Service Delivery Provider, then access and privacy provisions need to be considered in the contract or agreement.

2. Physical transfer of general records and personal information

Where the government organization decides to transfer its general records and personal information, all reasonable steps should be taken to protect the security and confidentiality of the information during its storage, transportation, and handling.

3. Outstanding Requests and Appeals

Government organizations should include procedures to deal with outstanding requests and appeals during the transition phase, prior to the contracting entity taking full custody or control of the government organization's general records or personal information.

For your convenience and ease of use the IPC has developed the following template that can be applied in preparing the agreement.

Model Access and Privacy Agreement

Note: This model agreement would be appropriate in those circumstances where a government organization **does not** retain custody or control of its general records or personal information. However, where the government organization does maintain custody or control of its records, there should be a clause in the agreement which stipulates that the contracting entity agrees to comply with the provisions of the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts)* in the course of providing services. For more information about circumstances where the government organization does retain custody or control of its records, please refer to Management Board's FIPPA Considerations for Alternative Services Delivery and the IPC's Investigation Report I97-017P.

AGREEMENT

[Indicate the title of the agreement]

I. Purpose

The purpose of this agreement is to establish policies and procedures regarding public access to general records held by the organization and the protection of personal information including access by individuals to their own personal information.

II. Definitions

'Access to information' means access by the public to the organization's general records.

The **'Access and Privacy Agreement'** means the policies and procedures dealing with access to information and the protection of privacy affixed to this agreement or contract.

'Personal Information' means information about an identifiable individual recorded in any form including:

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

c) any identifying number, symbol or other particular assigned to the individual;

d) the address, telephone number, fingerprints or blood type of the individual;

e) the personal opinions or views of the individual except where they relate to another individual;

f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the individual; and

h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

For the purpose of collection, 'personal information' includes information that is not recorded and that is otherwise defined as 'personal information' in this agreement.

The **'organization'** means... [name of the government organization].

III. Policies

1. Accountability and Administration

a) The [organization] shall develop and implement policies and procedures dealing with public access to information and the protection of privacy. The policies and procedures shall be publicly accessible.

b) The [organization] shall appoint a senior officer who shall have the responsibility of ensuring the organization's compliance with this agreement.

c) The [organization] shall develop a procedure and time frames for complying with requests for access to information already held by the [organization].

d) Staff will be required to adhere to strict confidentiality of personal information.

e) The [organization] shall publish information regarding its policies and procedures relating to the management of personal information and general records. Such information shall include:

  i) the name of the person responsible for the [organization]'s policies and procedures;

  ii) the name of the person to whom complaints should be directed;

  iii) the form such complaints should take;

  iv) the means of gaining access to personal information held by the [organization];

  v) a description of the type of personal information held by the [organization]; and

  vi) brochures or other documentation describing the [organization]'s policies, procedures and codes.

f) The [organization] shall ensure that the staff of the [organization] are adequately trained in order to ensure that the policies and procedures can be effectively implemented.

2.Protection of Personal Information

Collection

The collection of personal information shall be limited to that which is necessary for the [organization] to comply with the contract, or to meet the obligations of a statute. Wherever possible, personal information shall be collected directly from the individual to whom the information relates by fair and lawful means.

The purpose for which information is collected shall be identified by the [organization] to an individual, at or before the time the information is collected.

Individual Access

a) Upon request, the [organization] shall provide an individual with information concerning the existence, use and disclosure of his or her personal information and provide the applicable personal information to the individual, except where releasing the personal information would:

    i) violate another individual's right to privacy, unless that individual consents to the information's release;

    ii) violate solicitor-client privilege; or

    iii) compromise security, or legally recognized commercial proprietary concerns.

b) Personal information shall be made available to requesters at minimal or no cost and shall be provided in a form that is easily understandable.

Use and Disclosure

a) Personal information shall not be used or disclosed for purposes other than that for which it was collected, except with the consent of the individual or as required by law.

b) An individual's consent must be obtained before personal information may be disclosed to third parties, except for law enforcement purposes.

c) The [organization] shall provide personal information to third parties who can demonstrate that they have in place a means to provide protection comparable to that provided by the [organization].

d) Where personal information is made available to third parties on an ongoing basis, amendments to such information shall regularly be provided to them.

Consent

The knowledge and consent of the individual are required for the use, or disclosure of personal information, except where permitted under freedom of information and privacy legislation, such as law enforcement purposes.

Retention

a) Personal information shall be retained only as long as necessary for the fulfilment of the purpose for which it was collected.

b) Guidelines shall be developed to govern the period of time personal information is retained by the [organization].

Disposal

a) Reasonable steps should be taken to protect the security and confidentiality of personal information that is to be destroyed.

b) Personal information that is no longer required to fulfil the identified purposes should be permanently erased, rendered anonymous or destroyed in such a way that it cannot be reconstructed or retrieved.

d) Guidelines shall be developed and procedures implemented to govern the secure destruction of personal information to ensure it cannot be reconstructed or retrieved.

Accuracy

Personal information shall be as accurate, complete, and as up-to-date as possible.

Right of Correction

a) The individual has the right to ask that information relating to him or her be corrected, and where there is disagreement about the correctness of the information, the [organization] shall attach the individual's statement of disagreement to the personal information.

b) The individual may require that any third party to whom their personal information was disclosed, within the year before the time the correction was requested or a statement of disagreement required, be notified of the correction or statement of disagreement.

Security

In order to prevent the unauthorized disclosure, copying, use or modification of personal information held by the [organization], access to such information shall be restricted by the use of recognized security mechanisms such as passwords, encryption or other reasonable safeguards.

Complaints

a) An individual shall be able to file a complaint concerning compliance with the above rules to the designated individual or individuals accountable for the [organization's] compliance with this agreement.

b) The [organization] shall develop a mechanism to address all complaints about the handling of personal information and the refusal to grant access in response to a request for one's own information.

c) If a complaint is found to be justified, the [organization] shall take appropriate measures to rectify the problem in a timely manner.

d) The [organization] shall develop and implement procedures which establish a mechanism to allow any unresolved complaints to be addressed by an independent third party.

Penalties

No person shall willfully use, disclose, or retain personal information obtained under the authority of this agreement or contract, as determined by the [organization]'s enabling legislation.

3. Access to Information

Records of the [organization] shall be made available to the public on request, subject to the following exceptions:

i) personal information, including medical information, when the personal information is sought by persons other than by the individual to whom the information relates;

ii) law enforcement information;

iii) information, the disclosure of which, would violate solicitor-client privilege; and

iv) a trade secret, commercial, technical, financial, or labour relations information which, if released, would harm the competitive position of the [organization].

APPENDIX D

Best Practices for Protecting Individual Privacy in Conducting Survey Research (Full Version)

Best Practices for Protecting Individual Privacy in Conducting Survey Research

(Full Version)

April 1999

Information and Privacy
Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

This publication is also available on the IPC Web site. Upon request, this publication will be made available on audio tape.

Foreword

In 1998, the Ontario Provincial Service Restructuring Secretariat asked ministries to assess their services to the public and to subsequently develop action plans to improve any detected service gaps. Given the anticipated volume of survey research and that survey research may involve the collection, retention, use, disclosure, and disposal of personal information, the Information and Privacy Commissioner collaborated with the Ministry of Labour and the Corporate Freedom of Information and Privacy Office of Management Board Secretariat to develop best practices for protecting individual privacy in conducting survey research.

We would like to thank the following individuals for their contribution in developing this paper and the best practices:

Ministry of Labour

Peter Inokai, Chief Administrative Officer
Christopher Berzins, Manager, Freedom of Information & Privacy
Ron Brittain, Director, Information and Technology Management Branch

Corporate Freedom of Information and Privacy Office, Management Board Secretariat

Guy Herriges, Corporate Program Manager
Elizabeth Flavelle, Policy Adviser

Information and Privacy Commissioner/Ontario

Tom Mitchinson, Assistant Commissioner
Diane Frank, Manager of Mediation
Debra Grant, Research Officer
Linda Mariconda, Mediator

Introduction

As government institutions strive to become more efficient, accountable and customer focussed, they are more frequently seeking input from the public about their programs and services. One of the most cost-effective ways to elicit this input is through survey research.

Survey research can be used to help plan new programs and services or modify existing programs or services or the manner in which they are delivered, and to help ensure that the programs and services that are provided meet the needs and expectations of customers. Survey research can be used to obtain input from a wide range of individuals, including the direct or potential recipients of programs and services, the staff and managers responsible for planning and delivering programs and services, the taxpayers who provide the funding, and the public at large.

However, while survey research can be an important tool for shaping government programs and services, it may involve the collection, retention, use, disclosure, and disposal of personal information. *Personal information* is defined under the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*) as "recorded information about an identifiable individual." Personal information includes, for example, an individual's name, address, telephone number, age, sex, and his or her personal opinions or views.

Whenever provincial and local government institutions collect, retain, use, disclose, or dispose of personal information, they are required to comply with the privacy protection provisions of the *Acts*, and their regulations. To help institutions comply with the *Acts*, this paper details the privacy considerations at each stage in the design and implementation of survey research projects and recommends some best practices.

Survey research raises two central privacy considerations. The first is the potential collection of personal information from survey research participants. The second is the potential use of previously collected personal information for the purpose of obtaining a sample of survey research participants. With respect to the first consideration, the position advocated in the paper is that most survey research can be carried out anonymously and personally identifiable survey data is only required in very limited and specific circumstances. To the extent that the collection of personal information can be avoided, the privacy considerations will be minimized. However, with respect to the second consideration, it is often not possible to avoid the use of personal information altogether. Even where survey research is conducted anonymously, personal information may still be needed to obtain a sample of survey research participants. Therefore, individual privacy and compliance with the *Acts* will be a consideration in most cases.

For the purposes of the paper, the process of conducting survey research projects has been divided into eight stages:

- issue definition;
- research design and questionnaire development;
- pre-testing;
- sample selection;
- data collection;
- data analysis;
- reporting of results; and
- data archiving.

For the purposes of the paper, where the *Acts* are cited, the sections of the provincial *Act* appear first, followed by a slash (/) and the corresponding sections of the municipal *Act*, e.g., 38(2)/28(2).

For those individuals who are not familiar with the relevant provisions of the *Acts* cited in this paper, your institution's Freedom of Information and Privacy Coordinator will be able to assist you in complying with the requirements of the legislation in developing and conducting surveys.

For a short overview of this paper, or a summary of the recommendations, respectively refer to the *Condensed Version* or the *Summary of Best Practices*, both of which have been published in conjunction with *Best Practices for Protecting Individual Privacy in Conducting Survey Research*.

M121

IMPORTANT NOTE CONCERNING THE FOLLOWING PAGES

THE PAGES WHICH FOLLOW HAVE BEEN FILMED TWICE IN ORDER TO OBTAIN THE BEST REPRODUCTIVE QUALITY

USERS SHOULD CONSULT ALL THE PAGES REPRODUCED ON THE FICHE IN ORDER TO OBTAIN A COMPLETE READING OF THE TEXT.

REMARQUE IMPORTANTE CONCERNANT LES PAGES QUI SUIVENT

LES PAGES SUIVANTES ONT ÉTÉ REPRODUITES EN DOUBLE AFIN D'AMÉLIORER LA QUALITÉ DE REPRODUCTION

LES UTILISATEURS DOIVENT CONSULTER TOUTES LES PAGES REPRODUITES SUR LA FICHE AFIN D'OBTENIR LA LECTURE DU TEXTE INTÉGRAL

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

Privacy Considerations at Each Stage of a Survey Research Project

Stage 1: Issue Definition

Before developing a survey, it is important to clearly define the issue(s) you wish to address through the survey. In doing so, you must assess the purpose(s) and focus of the survey. For example, is the purpose to gather information to help plan new programs or services, to identify gaps in existing program/service delivery, etc.?

Clearly defining the purpose(s) of the survey will help limit the collection of information to that which is strictly necessary. In survey research that requires the collection of personal information, a clear understanding of the purposes of the survey will help to minimize the collection of personal information.

Under sections 39(2)(b)/29(2)(b) of the *Acts*, whenever personal information is collected, an institution is required to inform the individual to whom the information relates of the principle purpose or purposes for which the personal information will be used. In general, once the individual has been informed of the purposes for the collection, the collection, use and disclosure of that information should be limited to that which is necessary to fulfill the specified purposes. Thus, clearly defining the purposes of the survey is a precondition for determining what information needs to be collected, and how that information may be subsequently used and disclosed.

Best Practice #1

Clearly define the issues you wish to address. This will help to limit the collection of information to that which is necessary to address the issues at hand.

Stage 2: Research Design and Questionnaire Development

During the early stages of designing a survey, a number of key issues which may have implications for privacy protection need to be resolved. These issues include deciding who will conduct the survey, whether it will be necessary to collect personal information, whether you have the legal authority to collect the personal information, and the most appropriate type of survey research method to use.

Privacy Considerations at Each Stage of a Survey Research Project

Stage 1: Issue Definition

Before developing a survey, it is important to clearly define the issue(s) you wish to address through the survey. In doing so, you must assess the purpose(s) and focus of the survey. For example, is the purpose to gather information to help plan new programs or services, to identify gaps in existing program/service delivery, etc.?

Clearly defining the purpose(s) of the survey will help limit the collection of information to that which is strictly necessary. In survey research that requires the collection of personal information, a clear understanding of the purposes of the survey will help to minimize the collection of personal information.

Under sections 39(2)(b)/29(2)(b) of the *Acts*, whenever personal information is collected, an institution is required to inform the individual to whom the information relates of the principle purpose or purposes for which the personal information will be used. In general, once the individual has been informed of the purposes for the collection, the collection, use and disclosure of that information should be limited to that which is necessary to fulfill the specified purposes. Thus, clearly defining the purposes of the survey is a precondition for determining what information needs to be collected, and how that information may be subsequently used and disclosed.

Best Practice #1

Clearly define the issues you wish to address. This will help to limit the collection of information to that which is necessary to address the issues at hand.

Stage 2: Research Design and Questionnaire Development

During the early stages of designing a survey, a number of key issues which may have implications for privacy protection need to be resolved. These issues include deciding who will conduct the survey, whether it will be necessary to collect personal information, whether you have the legal authority to collect the personal information, and the most appropriate type of survey research method to use.

Who Will Conduct the Survey?

At some point during the survey research project, you need to decide whether the survey will be conducted by internal staff, by staff of another provincial or local government institution, or by external consultants. Regardless of who conducts the research, the same privacy protection rules should apply to any personal information that may be involved.

Whenever staff of an institution conduct survey research, Terms of Reference should set out the requirements for the collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. (A sample Terms of Reference is contained in Appendix A.) Whenever external consultants or private companies conduct survey research, they are collecting information on behalf of an institution and, as agents of the institution, are subject to the same privacy protection requirements as any other employees of institutions. In such cases, contractual agreements should be established to clarify external consultants' obligations to collect, retain, use, disclose and dispose of personal information, in accordance with the *Acts*. Contractual agreements should also ensure institutions retain control over any personal information that may be involved in survey research. (A sample agreement is contained in Appendix B.)

It is important that you review either the Terms of Reference or the contractual agreement periodically during the survey and at the completion of it, to ensure that all conditions set out in either document have been fully complied with.

Best Practice #2

Where staff of your institution or another institution conduct the survey, prepare Terms of Reference setting out the requirements for the collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. (See Appendix A for a sample Terms of Reference.)

Best Practice #3

Where an external consultant or private company conducts the research, establish a contractual agreement to ensure that personal information is collected, retained, used, disclosed and disposed of in accordance with the *Acts*. (See Appendix B for a sample agreement of such terms and conditions.)

Best Practice #4

Review either the Terms of Reference or the contractual agreement periodically during the survey and at the completion of it, to ensure that all conditions set out in either document have been fully complied with.

Try to Avoid Collecting Personal Information

During the early stages of research design, determine what personal information, if any, needs to be collected from survey research participants. This is an important issue to consider up-front, because if you want to collect personal information, you must first ensure that you have the authority to do so under the *Acts*. This collection issue should not be confused with the issue of using personal information that has previously been collected by your institution to select a survey research sample. That is a separate issue that will be addressed in Stage 4.

Determining whether you need to collect personal information, as defined under the *Acts*, may not be straightforward. In making this determination, consider who will be included in the target population, the nature of the information that will be requested from participants, and the extent to which the survey responses will identify or could be used to identify an individual.

The views and opinions elicited by the survey may not clearly fall within the definition of personal information. For example, if the survey has been designed to elicit the views and opinions of employees or groups of professionals, such as doctors, the information may not fall under the definition of personal information.

Various orders of the Information and Privacy Commissioner (IPC) have found that, in general, the views and opinions expressed in an individual's professional capacity are not the individual's personal information. Institutions are not required to comply with the privacy protection provisions of the *Acts* with respect to information that clearly falls outside the definition of personal information. If there is any ambiguity about whether the information is personal information, err on the side of caution by complying with the *Acts*.

Also, regardless of whether information is defined as personal information for the purposes of the *Acts*, survey participants may have concerns about the manner in which their views and opinions expressed through the survey research are used and disclosed. Therefore, whenever possible, conduct surveys anonymously (i.e., so that the survey responses do not identify and cannot be used to identify an individual). Conducting surveys anonymously is the best way of ensuring the privacy of survey participants.

Who Will Conduct the Survey?

At some point during the survey research project, you need to decide whether the survey will be conducted by internal staff, by staff of another provincial or local government institution, or by external consultants. Regardless of who conducts the research, the same privacy protection rules should apply to any personal information that may be involved.

Whenever staff of an institution conduct survey research, Terms of Reference should set out the requirements for the collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. (A sample Terms of Reference is contained in Appendix A.) Whenever external consultants or private companies conduct survey research, they are collecting information on behalf of an institution and, as agents of the institution, are subject to the same privacy protection requirements as any other employees of institutions. In such cases, contractual agreements should be established to clarify external consultants' obligations to collect, retain, use, disclose and dispose of personal information, in accordance with the *Acts*. Contractual agreements should also ensure institutions retain control over any personal information that may be involved in survey research. (A sample agreement is contained in Appendix B.)

It is important that you review either the Terms of Reference or the contractual agreement periodically during the survey and at the completion of it, to ensure that all conditions set out in either document have been fully complied with.

Best Practice #2

Where staff of your institution or another institution conduct the survey, prepare Terms of Reference setting out the requirements for the collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. (See Appendix A for a sample Terms of Reference.)

Best Practice #3

Where an external consultant or private company conducts the research, establish a contractual agreement to ensure that personal information is collected, retained, used, disclosed and disposed of, in accordance with the *Acts*. (See Appendix B for a sample agreement of related terms and conditions.)

Best Practice #4

Review either the Terms of Reference or the contractual agreement periodically during the survey and at the completion of it, to ensure that all conditions set out in either document have been fully complied with.

Try to Avoid Collecting Personal Information

During the early stages of research design, determine what personal information, if any, needs to be collected from survey research participants. This is an important issue to consider up-front, because if you want to collect personal information, you must first ensure that you have the authority to do so under the *Acts*. This collection issue should not be confused with the issue of using personal information that has previously been collected by your institution to select a survey research sample. That is a separate issue that will be addressed in Stage 4.

Determining whether you need to collect personal information, as defined under the *Acts*, may not be straightforward. In making this determination, consider who will be included in the target population, the nature of the information that will be requested from participants, and the extent to which the survey responses will identify or could be used to identify an individual.

The views and opinions elicited by the survey may not clearly fall within the definition of personal information. For example, if the survey has been designed to elicit the views and opinions of employees or groups of professionals, such as doctors, the information may not fall under the definition of personal information.

Various orders of the Information and Privacy Commissioner (IPC) have found that, in general, the views and opinions expressed in an individual's professional capacity are **not** the individual's personal information. Institutions are not required to comply with the privacy protection provisions of the *Acts* with respect to information that clearly falls outside the definition of personal information. If there is any ambiguity about whether the information is personal information, err on the side of caution by complying with the *Acts*.

Also, regardless of whether information is defined as personal information for the purposes of the *Acts*, survey participants may have concerns about the manner in which their views and opinions expressed through the survey research are used and disclosed. Therefore, whenever possible, conduct surveys anonymously (i.e., so that the survey responses do not identify and cannot be used to identify an individual). Conducting surveys anonymously is the best way of ensuring the privacy of survey participants.

Best Practice #5

Determine early in the design of your survey if it is necessary to collect personal information, as defined in the *Acts*. If you are uncertain as to whether the information in question is personal information, contact your institution's Freedom of Information and Privacy Co-ordinator or a Policy Advisor at Management Board Secretariat's Corporate Freedom of Information and Privacy Office. If personal information will be collected, you must comply with the privacy protection provisions of the *Acts*.

Anonymous Surveys

In designing any survey, always consider the possibility of collecting information such that the survey data do not identify and cannot be used to identify an individual. To the extent that the survey can be conducted anonymously, the risk of unauthorized and/or inappropriate collection, use and disclosure of personal information will be kept to a minimum. Moreover, in conducting anonymous surveys, compliance with the *Acts* is not required.

While anonymous surveys may be ideal from a privacy perspective, they present a number of research design challenges. One challenge is that, since there is no way of knowing who has responded to an anonymous survey, it will be difficult to follow-up with those individuals who do not respond. A lack of follow-up could result in a poor response rate and, consequently, the validity of the results of the survey could be questioned. However, to help ensure an adequate response rate, follow-up could be accomplished by contacting all potential participants regardless of whether they responded.

Alternatively, participants could be provided with another means of indicating that they had responded (e.g., they could mail in a postcard containing their name or some other personal identifier indicating that they had responded, at the same time as they mail in their anonymous questionnaire). Then, follow-up could be carried out with only those participants who have not yet confirmed that they have responded.

Another challenge is that anonymous surveys do not permit verification or clarification of information provided by survey participants. In addition, anonymous survey data cannot be linked to information obtained in successive surveys or to information available through other sources such as a client or customer database. While this will not be an issue in most survey research, in some circumstances there may be a clear rationale for linking information across time and/or sources or for following-up with participants.

Best Practice #6

If possible, design a survey so that the information collected does not identify and cannot be used to identify an individual (i.e., an anonymous survey).

Coded Surveys

An alternative to having completely anonymous survey responses would be to replace all personally identifiable data in the survey with a special code. This special code should not, in and of itself, identify the individual but should be used to link the survey data with personal information for limited and specific purposes (i.e., to facilitate follow-up and the linking of information across time and sources).

The survey data with the special code should be retained separately from the personal information that identifies participants. The only link between the two sets of data should be the special code. Access to the personal information through the special code should be limited to those individuals with a need-to-know for specific purposes, as outlined above.

If the survey is to be coded in this manner, potential participants should be informed of this procedure and its purpose prior to participation in the survey. Also, survey data with this type of coding falls within the definition of personal information. Therefore, you are required to comply with the *Acts* with respect to the collection, retention, use, disclosure, and disposal of this information.

Best Practice #7

If the survey cannot be carried out anonymously, design it so that all personal information is replaced with a special code that can only be used to link the survey data to personal information when it is necessary to do so (i.e., a coded survey).

Best Practice #8

When conducting a coded survey, be sure to:

- **inform potential participants about this procedure and its purpose;**
- **retain the coded survey data separately from the personal information; and**
- **limit the number of people who are able to relink the survey responses with the personal information.**

Personal Information Not Directly Related to the Survey

In some cases, you may want to collect personal information at the same time that you collect responses to the survey for a purpose not directly related to the current survey. For example, you may want survey participants to provide personal information, such as name, address and/or telephone number, so that you may provide them with information about the programs or services offered by your institution, provide them with a summary of the survey results or contact them as potential participants in subsequent research projects.

Best Practice #

Determine early in the design of your survey if it is necessary to collect personal information, as defined in the *Acts*. If you are uncertain as to whether the information in question is personal information, contact your institution's Freedom of Information and Privacy Co-ordinator or a Policy Advisor at Management Board Secretariat's Corporate Freedom of Information and Privacy Office. If personal information will be collected, you must comply with the privacy protection provisions of the *Acts*.

Anonymous Surveys

In designing any survey, always consider the possibility of collecting information such that the survey data do not identify and cannot be used to identify an individual. To the extent that the survey can be conducted anonymously, the risk of unauthorized and/or inappropriate collection, use and disclosure of personal information will be kept to a minimum. Moreover, in conducting anonymous surveys, compliance with the *Acts* is not required.

While anonymous surveys may be ideal from a privacy perspective, they present a number of research design challenges. One challenge is that, since there is no way of knowing who has responded to an anonymous survey, it will be difficult to follow-up with those individuals who do not respond. A lack of follow-up could result in a poor response rate and, consequently, the validity of the results of the survey could be questioned. However, to help ensure an adequate response rate, follow-up could be accomplished by contacting all potential participants regardless of whether they responded.

Alternatively, participants could be provided with another means of indicating that they had responded (e.g., they could mail in a postcard containing their name or some other personal identifier indicating that they had responded, at the same time as they mail in their anonymous questionnaire). Then, follow-up could be carried out with only those participants who have not yet confirmed that they have responded.

Another challenge is that anonymous surveys do not permit verification or clarification of information provided by survey participants. In addition, anonymous survey data cannot be linked to information obtained in successive surveys or to information available through other sources such as a client or customer database. While this will not be an issue in most survey research, in some circumstances there may be a clear rationale for linking information across time and/or sources or for following-up with participants.

[illegible]

Coded Surveys

An alternative to having completely anonymous survey responses would be to replace all personally identifiable data in the survey with a special code. This special code should not, in and of itself, identify the individual but should be used to link the survey data with personal information for limited and specific purposes (i.e., to facilitate follow-up and the linking of information across time and sources).

The survey data with the special code should be retained separately from the personal information that identifies participants. The only link between the two sets of data should be the special code. Access to the personal information through the special code should be limited to those individuals with a need-to-know for specific purposes, as outlined above.

If the survey is to be coded in this manner, potential participants should be informed of this procedure and its purpose prior to participation in the survey. Also, survey data with this type of coding falls within the definition of personal information. Therefore, you are required to comply with the *Acts* with respect to the collection, retention, use, disclosure, and disposal of this information.

Best Practice #7

If the survey cannot be carried out anonymously, design it so that all personal information is replaced with a special code that can only be used to link the survey data to personal information when it is necessary to do so (i.e., a coded survey).

Best Practice #8

When conducting a coded survey, be sure to:

- inform potential participants about this procedure and its purpose;
- retain the coded survey data separately from the personal information; and
- limit the number of people who are able to relink the survey responses with the personal information.

Personal Information Not Directly Related to the Survey

In some cases, you may want to collect personal information at the same time that you collect responses to the survey for a purpose not directly related to the current survey. For example, you may want survey participants to provide personal information, such as name, address and/or telephone number, so that you may provide them with information about the programs or services offered by your institution, provide them with a summary of the survey results or contact them as potential participants in subsequent research projects.

In such cases, since there is really no need to link the personal information to the survey responses, survey participants should not be asked to provide this information with their responses. To ensure that there is no possibility of the survey responses being linked to the personal information, the two types of information should be collected separately. For example, survey participants could be provided with a separate postcard containing their personal information (i.e., name, address and/or telephone number) to mail to your institution indicating their desire for a summary of the survey results.

Best Practice #9

When collecting personal information at the same time as the survey responses, for a purpose not directly related to the survey, keep the two types of information completely separate.

If You Need to Collect Personal Information, Do You Have the Authority?

If you determine that it will be necessary to collect personal information in the course of conducting a survey, assess whether you have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*.

Sections 38(2)/28(2) set out the conditions under which personal information may be collected. Specifically, they state: "No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity."

If one of these three conditions does **not** exist, you do **not** have the authority to collect the personal information under the *Acts*. Where you determine that you do not have the authority to collect, you should consider conducting an anonymous survey, as discussed previously.

Best Practice #10

Determine whether you have the authority to collect the personal information required for the survey, under sections 38(2)/28(2) of the *Acts*.

Best Practice #11

Limit the amount of personal information collected in the survey to what is strictly necessary.

Determine the Most Appropriate Survey Research Method

In designing your survey, select a survey research method that will elicit the desired information from survey respondents (e.g., mail, telephone, personal interviews, focus groups, e-mail, Internet Web site, disk-by-mail). However, some methods are more intrusive than others. For example, receiving a questionnaire in the mail may be less intrusive than a telephone survey.

The nature of the information to be requested in the survey should be considered when determining the most appropriate method to use. For example, you would probably not choose a telephone survey to elicit sensitive information about an individual's health, but rather, a less intrusive method, such as an anonymous questionnaire.

Best Practice #12

Select a survey research method that complements the degree of sensitivity of the information to be collected.

Stage 3: Pretesting (fine-tuning) the Survey

When you pretest the survey, you may collect personal information about pretest participants. Therefore, apply the best practices discussed in this paper to any personal information collected during the pre-test phase of the project.

Best Practice #13

Treat any personal information collected during the pretest in the same manner as you would treat personal information collected through the survey.

Stage 4: Sample Selection

Even if a survey is conducted anonymously, you may still need to collect or use personal information to obtain a survey research sample. The sample can be obtained in a number of ways depending on the purposes for conducting the survey. Some of the more common methods of obtaining a survey research sample are as follows:

- by contacting those individuals with whom your institution has had direct contact in the context of the programs or services that it provides (i.e., using the personal information previously collected from your direct customers or clients);

In such cases, since there is really no need to link the personal information to the survey responses, survey participants should **not** be asked to provide this information with their responses. To ensure that there is no possibility of the survey responses being linked to the personal information, the two types of information should be collected separately. For example, survey participants could be provided with a separate postcard containing their personal information (i.e., name, address and/or telephone number) to mail to your institution indicating their desire for a summary of the survey results.

Best Practice #9

When collecting personal information at the same time as the survey responses, for a purpose not directly related to the survey, keep the two types of information completely separate.

If You Need to Collect Personal Information, Do You Have the Authority?

If you determine that it will be necessary to collect personal information in the course of conducting a survey, assess whether you have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*.

Sections 38(2)/28(2) set out the conditions under which personal information may be collected. Specifically, they state: "No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity."

If one of these three conditions does **not** exist, you do **not** have the authority to collect the personal information under the *Acts*. Where you determine that you do not have the authority to collect, you should consider conducting an anonymous survey, as discussed previously.

Best Practice #10

Determine whether you have the authority to collect the personal information required for the survey, under sections 38(2)/28(2) of the *Acts*.

Best Practice #11

Limit the amount of personal information collected for the survey to what is strictly necessary.

Determine the Most Appropriate Survey Research Method

In designing your survey, select a survey research method that will elicit the desired information from survey respondents (e.g., mail, telephone, personal interviews, focus groups, e-mail, Internet Web site, disk-by-mail). However, some methods are more intrusive than others. For example, receiving a questionnaire in the mail may be less intrusive than a telephone survey.

The nature of the information to be requested in the survey should be considered when determining the most appropriate method to use. For example, you would probably not choose a telephone survey to elicit sensitive information about an individual's health, but rather, a less intrusive method, such as an anonymous questionnaire.

Best Practice #12

Select a survey research method that complements the degree of sensitivity of the information to be collected.

Stage 3: Pretesting (fine-tuning) the Survey

When you pretest the survey, you may collect personal information about pretest participants. Therefore, apply the best practices discussed in this paper to any personal information collected during the pre-test phase of the project.

Best Practice #13

Treat any personal information collected during the pretest in the same manner as you would treat personal information collected through the survey.

Stage 4: Sample Selection

Even if a survey is conducted anonymously, you may still need to collect or use personal information to obtain a survey research sample. The sample can be obtained in a number of ways depending on the purposes for conducting the survey. Some of the more common methods of obtaining a survey research sample are as follows:

- by contacting those individuals with whom your institution has had direct contact in the context of the programs or services that it provides (i.e., using the personal information previously collected from your direct customers or clients);

- by contacting those individuals on a list obtained from another institution or third party (i.e., indirectly collecting personal information that was previously collected by another institution or third party); and
- by asking another institution or third party to contact individuals on your behalf (i.e., by having another institution or third party use personal information previously collected from its customers or clients).

Depending on which method is used to obtain your survey research sample, different privacy issues need to be addressed. The privacy considerations associated with each method are discussed below.

Using Personal Information Previously Collected from your Customers or Clients

In conducting surveys of your direct customers or clients, you will need to use personal information that has already been collected from them to obtain the survey research sample. Usually, personal information, such as name, address, and/or telephone number, is only needed to contact potential survey participants. However, in some cases, additional personal information (e.g., age, gender, education, and income) may be needed to select a sample with specific characteristics. In most cases, this client or customer information would have been collected within the context of delivering the programs or services that are the focus of the survey.

Providing Notice at the Time of Collection

If you anticipate in advance that customer or client information will be used to obtain a survey research sample, then the appropriate notice of this use should be provided at the time of collection.

Sections 39(2)/29(2) of the *Acts* state that where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of:

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

M121

IMPORTANT NOTE CONCERNING THE FOLLOWING PAGES

THE PAGES WHICH FOLLOW HAVE BEEN FILMED TWICE IN ORDER TO OBTAIN THE BEST REPRODUCTIVE QUALITY

USERS SHOULD CONSULT ALL THE PAGES REPRODUCED ON THE FICHE IN ORDER TO OBTAIN A COMPLETE READING OF THE TEXT.

REMARQUE IMPORTANTE CONCERNANT LES PAGES QUI SUIVENT

LES PAGES SUIVANTES ONT ÉTÉ REPRODUITES EN DOUBLE AFIN D'AMÉLIORER LA QUALITÉ DE REPRODUCTION

LES UTILISATEURS DOIVENT CONSULTER TOUTES LES PAGES REPRODUITES SUR LA FICHE AFIN D'OBTENIR LA LECTURE DU TEXTE INTÉGRAL

micromedia
a division of IHS Canada

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca

Best Practice #14

Where you know in advance that customer or client information will be used to select a survey sample, provide notice of this use at the time of collection. (The subsequent use of the personal information for this purpose would be in compliance with sections 41(b)/31(b) of the *Acts*, since you would be using the personal information for the purpose intended at the time of collection.)

No Notice Provided at the Time of Collection

Although providing notice of the use of personal information for survey research purposes is always the best practice, in some circumstances the *Acts* may permit the use of personal information for this purpose even though no notice was provided at the time of collection.

Sections 41/31 of the *Acts* address the *use* of personal information. These sections state that an institution shall not use personal information except:

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose; or

(c) for a purpose for which the information may be disclosed to the institution under sections 42/32 of the *Acts*.

Under subsection (a), personal information could be used to select a survey research sample if the individual has consented to this use. However, in many cases it will not be reasonable or practical to obtain consent from every potential survey participant and you will have to assess whether you may use the personal information for this purpose under subsection (b).

In most customer or client surveys, the personal information that would be used to obtain a survey research sample would have been obtained within the context of providing the service or program which is the focus of the survey. The *Acts* state that where personal information has been collected *directly* from the individual to whom it relates, the purpose of a use of that information is a consistent purpose (sections 41(b)/31(b) of the *Acts*) only if the individual *might reasonably have expected* such a use (sections 43/33 of the *Acts*). Where personal information has been collected *indirectly* from another source, the purpose of a use of that information is a consistent purpose only if it is *reasonably compatible* with the purpose for which it was obtained or compiled.

Best Practice #14

Where you know in advance that customer or client information will be used to select a survey sample, provide notice of this use at the time of collection. (The subsequent use of the personal information for this purpose would be in compliance with sections 41(b)/31(b) of the *Acts*, since you would be using the personal information for the purpose intended at the time of collection.)

No Notice Provided at the Time of Collection

Although providing notice of the use of personal information for survey research purposes is always the best practice, in some circumstances the *Acts* may permit the use of personal information for this purpose even though no notice was provided at the time of collection.

Sections 41/31 of the *Acts* address the *use* of personal information. These sections state that an institution shall not use personal information except:

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose; or

(c) for a purpose for which the information may be disclosed to the institution under sections 42/32 of the *Acts*.

Under subsection (a), personal information could be used to select a survey research sample if the individual has consented to this use. However, in many cases it will not be reasonable or practical to obtain consent from every potential survey participant and you will have to assess whether you may use the personal information for this purpose under subsection (b).

In most customer or client surveys, the personal information that would be used to obtain a survey research sample would have been obtained within the context of providing the service or program which is the focus of the survey. The *Acts* state that where personal information has been collected *directly* from the individual to whom it relates, the purpose of a use of that information is a consistent purpose (sections 41(b)/31(b) of the *Acts*) only if the individual *might reasonably have expected* such a use (sections 43/33 of the *Acts*). Where personal information has been collected *indirectly* from another source, the purpose of a use of that information is a consistent purpose only if it is *reasonably compatible* with the purpose for which it was obtained or compiled.

Subsections 41(c)/31(c) do not apply when you obtain the survey sample through the use of information previously collected from your direct clients or customers. It may apply when the survey sample is obtained through the collection of information from another institution or third party, as discussed below.

Best Practice #15

Where you have not anticipated using personal information to select a survey sample at the time of collection, only use the information for this purpose if:

- **the individual consents to the use; or**
- **the use is consistent with the purpose for which the information was obtained or compiled.**

Collecting Personal Information from Another Institution or Third Party

In conducting surveys of individuals other than your direct customers or clients, you may wish to select your survey sample through the collection of personal information from another institution or third party. This is considered to be an *indirect collection* of personal information under the *Acts*.

Sections 39(1)/29(1) of the *Acts* require that personal information be collected directly from the individual to whom it relates, unless certain circumstances listed in sections 39(1)(a) to (h)/29(1)(a) to (h) exist (e.g., where the individual authorizes another manner of collection, where another manner of collection is authorized by or under a statute, etc.). If you intend to collect personal information other than directly from the individual, you must determine whether you have the authority to do so under sections 39(1)/29(1).

Sections 39(1)(c)/29(1)(c) permit the indirect collection of personal information where the Information and Privacy Commissioner has authorized this manner of collection under sections 59(c)/46(c). Sections 59(c)/46(c) state that the Commissioner may, in appropriate circumstances, authorize the collection of personal information other than directly from the individual. Where no other provisions in sections 39(1)/29(1) authorize this manner of collection, you should apply to the Commissioner for authorization. You can do this by completing an Application for Indirect Collection, available from the IPC.

Best Practice #16

Before collecting personal information indirectly from another institution or third party to obtain a survey research sample, assess your authority to do so under sections 39(1)/29(1) of the *Acts*.

Collecting Information from Public Records for Sample Selection

Public databases are one source of information that may be used to compile lists of potential research participants. A list of public databases can be found in Management Board Secretariat's annual Directory of Records. The list includes public databases such as the Personal Property Security Registration System and the Land Registration System maintained by the Ministry of Consumer and Commercial Relations.

Under sections 37/27 of the *Acts*, public databases are excluded from the privacy protection provisions of the *Acts*. The rationale for this exclusion is that there are legitimate needs for this information to be widely available to the general public, and imposing restrictions on the use and disclosure of this information under the *Acts* would not make sense. But, although public databases are excluded from the privacy provisions of the *Acts*, this does not mean that there are no privacy implications in the collection, use and disclosure of this information for unintended purposes without the knowledge and consent of individuals.

The privacy investigation reports of the IPC have generally found that under sections 37/27, personal information that is maintained by an institution may be excluded from the application of the *Acts* only if the personal information is maintained by that institution specifically for the purpose of creating a record which is available to the general public. Other institutions cannot claim the exclusion unless they also maintain the personal information for this purpose. Consequently, you may only collect personal information contained in a public database if you have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*.

Best Practice #17

The inclusion of personal information in a public database does not necessarily mean that you have the authority to collect that information to select a survey sample. Before collecting personal information from a public database for this purpose, assess whether you have the authority to do so under sections 38(2)/28(2) of the *Acts*.

Collecting Information from Another Institution's Personal Information Banks for Sample Selection

Another possible source of information that may be used to compile lists of potential research participants is the personal information maintained by other government institutions or other third parties. When institutions obtain a survey research sample in this manner, this is referred to as *data sharing*.

Subsections 41(c)/31(c) do not apply when you obtain the survey sample through the use of information previously collected from your direct clients or customers. It may apply when the survey sample is obtained through the collection of information from another institution or third party, as discussed below.

Best Practice #15

Where you have not anticipated using personal information to select a survey sample at the time of collection, only use the information for this purpose if:

- **the individual consents to the use; or**
- **the use is consistent with the purpose for which the information was obtained or compiled.**

Collecting Personal Information from Another Institution or Third Party

In conducting surveys of individuals other than your direct customers or clients, you may wish to select your survey sample through the collection of personal information from another institution or third party. This is considered to be an *indirect collection* of personal information under the *Acts*.

Sections 39(1)/29(1) of the *Acts* require that personal information be collected directly from the individual to whom it relates, unless certain circumstances listed in sections 39(1)(a) to (h)/29(1)(a) to (h) exist (e.g., where the individual authorizes another manner of collection, where another manner of collection is authorized by or under a statute, etc.). If you intend to collect personal information other than directly from the individual, you must determine whether you have the authority to do so under sections 39(1)/29(1).

Sections 39(1)(c)/29(1)(c) permit the indirect collection of personal information where the Information and Privacy Commissioner has authorized this manner of collection under sections 59(c)/46(c). Sections 59(c)/46(c) state that the Commissioner may, in appropriate circumstances, authorize the collection of personal information other than directly from the individual. Where no other provisions in sections 39(1)/29(1) authorize this manner of collection, you should apply to the Commissioner for authorization. You can do this by completing an Application for Indirect Collection, available from the IPC.

Best Practice #16

Before collecting personal information indirectly from another institution or third party to obtain a survey research sample, assess your authority to do so under sections 39(1)/29(1) of the *Acts*.

Collecting Information from Public Records for Sample Selection

Public databases are one source of information that may be used to compile lists of potential research participants. A list of public databases can be found in Management Board Secretariat's annual Directory of Records. The list includes public databases such as the Personal Property Security Registration System and the Land Registration System maintained by the Ministry of Consumer and Commercial Relations.

Under sections 37/27 of the *Acts*, public databases are excluded from the privacy protection provisions of the *Acts*. The rationale for this exclusion is that there are legitimate needs for this information to be widely available to the general public, and imposing restrictions on the use and disclosure of this information under the *Acts* would not make sense. But, although public databases are excluded from the privacy provisions of the *Acts*, this does not mean that there are no privacy implications in the collection, use and disclosure of this information for unintended purposes without the knowledge and consent of individuals.

The privacy investigation reports of the IPC have generally found that under sections 37/27, personal information that is maintained by an institution may be excluded from the application of the *Acts* only if the personal information is maintained by that institution specifically for the purpose of creating a record which is available to the general public. Other institutions cannot claim the exclusion unless they also maintain the personal information for this purpose. Consequently, you may only collect personal information contained in a public database if you have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*.

Best Practice #17

The inclusion of personal information in a public database does not necessarily mean that you have the authority to collect that information to select a survey sample. Before collecting personal information from a public database for this purpose, assess whether you have the authority to do so under sections 38(2)/28(2) of the *Acts*.

Collecting Information from Another Institution's Personal Information Banks for Sample Selection

Another possible source of information that may be used to compile lists of potential research participants is the personal information maintained by other government institutions or other third parties. When institutions obtain a survey research sample in this manner, this is referred to as *data sharing*.

4

The sharing of personal information between two organizations runs counter to two of the most fundamental principles of data protection — that personal information should be collected directly from the individual to whom it pertains, and should only be used for the purpose for which it was collected (with limited exceptions). Data sharing respects neither of these principles since the personal information is collected indirectly and used for a purpose for which it may not have been intended at the time of collection.

Data sharing between organizations may lead to individuals' loss of control over their personal information. Therefore, where possible, sharing should not occur without exploring less privacy-intrusive means of meeting the objectives of the survey. Before making a decision to share personal data, consider all practical alternatives which are more privacy protective. You should also consider the merits of any contemplated data sharing and whether sharing is appropriate.

Any sharing of personal information should be supported by a written *data sharing agreement*. Such an agreement will clarify the rights and obligations of all parties in a data sharing activity and thereby ensure compliance with the *Acts*. To prepare such an agreement, refer to the IPC's *Model Data Sharing Agreement*.

Among other things, the agreement should specify that the institution conducting the survey should assess whether it has the authority to collect the personal information in question. In addition, if the party maintaining the personal information bank is an institution subject to one of the *Acts*, it should assess whether it has the authority to use and disclose the personal information for this purpose, respectively, under sections 41/31 and 42/32 of the *Acts*.

One of the exceptions under sections 42/32 that an institution maintaining the personal information bank may rely on to disclose this personal information is subsection 42(a)/32(a), which states that an institution shall not disclose personal information in its custody or under its control except in accordance with Parts II/I. Subsections 21(1)(e)/14(1)(e) fall under Parts II/I and state that an institution may disclose personal information that identifies an individual to a person other than the individual to whom the information relates for a **research purpose**, when certain conditions are met. These conditions are:

- the disclosure must be consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained;
- the research purpose for which the disclosure is to be made cannot be reasonably achieved unless the information is provided in a form which allows individuals to be identified; and
- the person who is to receive the record must agree to comply with conditions relating to security and confidentiality prescribed by section 10(1) of Regulation 460/section 10(1) of Regulation 823.

One of the conditions set out in the Regulations is that the recipient of the information must obtain written authority from the institution maintaining the personal information in order to contact, either directly or indirectly, any individual to whom the personal information relates.

Section 10(2) of Reg. 460 and section 10(2) of Reg. 823 require that an agreement relating to the security and confidentiality of personal information to be disclosed for a research purpose be in *Form 1*, which is set out in the Regulations.

Best Practice #18

Before sharing data to select a survey sample, prepare a data sharing agreement as per the IPC's *Model Data Sharing Agreement*. Among other things, the agreement should stipulate that:

- **the institution conducting the survey must comply with sections 38(2)/28(2) of the *Acts* with respect to the authority to collect the personal information being shared;**
- **if the party maintaining the personal information bank is an institution subject to one of the *Acts*, it should assess whether it has the authority to use and disclose the personal information for this purpose, respectively, under sections 41/31 and 42/32 of the *Acts*.**

Obtaining Your Survey Research Sample Indirectly Through Another Institution or Third Party

In some cases, it may be possible to avoid collecting personal information to obtain a survey research sample. This could be done by asking another institution or third party to use the information that it maintains (e.g., information in a public database or personal information bank) to contact potential research participants directly on your behalf. For example, an institution or third party could be asked to mail the surveys directly to potential participants. If the survey is an anonymous survey, participants could be asked to return their anonymous surveys directly to the institution conducting the research. The institution conducting the survey would thereby avoid the collection of personal information altogether.

However, if the survey is not anonymous, the institution conducting the research must have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*. In addition, all potential participants should be provided with the proper notice of collection of personal information by the institution conducting the survey, as required under sections 39(2)/29(2) of the *Acts*.

One of the conditions set out in the Regulations is that the recipient of the information must obtain written authority from the institution maintaining the personal information in order to contact, either directly or indirectly, any individual to whom the personal information relates.

Section 10(2) of Reg. 460 and section 10(2) of Reg. 823 require that an agreement relating to the security and confidentiality of personal information to be disclosed for a research purpose be in *Form 1*, which is set out in the Regulations.

Best Practice #18

Before sharing data to select a survey sample, prepare a data sharing agreement as per the IPC's *Model Data Sharing Agreement*. Among other things, the agreement should stipulate that:

- **the institution conducting the survey must comply with sections 38(2)/ 28(2) of the *Acts* with respect to the authority to collect the personal information being shared;**
- **if the party maintaining the personal information bank is an institution subject to one of the *Acts*, it should assess whether it has the authority to use and disclose the personal information for this purpose, respectively, under sections 41/31 and 42/32 of the *Acts*.**

Obtaining Your Survey Research Sample Indirectly Through Another Institution or Third Party

In some cases, it may be possible to avoid collecting personal information to obtain a survey research sample. This could be done by asking another institution or third party to use the information that it maintains (e.g., information in a public database or personal information bank) to contact potential research participants directly on your behalf. For example, an institution or third party could be asked to mail the surveys directly to potential participants. If the survey is an anonymous survey, participants could be asked to return their anonymous surveys directly to the institution conducting the research. The institution conducting the survey would thereby avoid the collection of personal information altogether.

However, if the survey is not anonymous, the institution conducting the research must have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*. In addition, all potential participants should be provided with the proper notice of collection of personal information by the institution conducting the survey, as required under sections 39(2)/29(2) of the *Acts*.

Regardless of whether the survey is conducted anonymously, the institution maintaining the information must assess whether it has the authority, under sections 41/31 of the *Acts*, to use the information to contact potential research participants (on behalf of the institution conducting the research).

Best Practice #19

If possible, avoid collecting personal information to obtain a survey research sample, by having the institution or third party that maintains the personal information contact potential research participants directly on your behalf.

Best Practice #20

Before using personal information to contact potential research participants on behalf of another institution or third party, assess whether you are authorized to use the information for this purpose, under sections 41/31 of the *Acts*.

Implications for Personal Information Banks

Regardless of whether notice was provided at the time of collection, if you use personal information to obtain a survey research sample, ensure that you comply with the requirements for personal information banks set out under sections 44 to 46 of the provincial *Act*, and sections 34 and 35 of the municipal *Act*. A *personal information bank* consists of personal information under your institution's control that is organized or intended to be retrieved by the individual's name or by an identifying number, symbol or other particular assigned to the individual.

If the personal information of customers or clients is to be used for survey research purposes on a regular basis, then this should be specified in the index of personal information banks, as required under subsections 45(d)/34(1)(d) of the *Acts*. Where the use has not been included in the index of personal information banks, sections 46(1)(a)/35(1)(a) of the *Acts* require that you attach or link to the personal information a record of this use. In addition, if the use has not been included in the index, section 46(3) of the provincial *Act* requires that the responsible minister be notified and the use be included in the index in the future. Under section 34(2) of the municipal *Act*, you must ensure that the index is amended as required to ensure its accuracy.

Best Practice #21

When using personal information to select a survey research sample, comply with the requirements for personal information banks set out under sections 44 to 46 of the provincial *Act*, or sections 34 and 35 of the municipal *Act*.

Stage 5: Data Collection

Contacting Potential Participants in the Survey

The fact that an individual has received one of your institution's programs or services could be considered to be sensitive personal information. When contacting potential survey participants, ensure that you do not invade their privacy by inadvertently disclosing this information to third parties, such as family members or co-workers.

For example, when contacting potential participants by mail, your institution name should not be printed on the outside of the envelope, as this information could reveal to others residing in the household that the individual has some relationship with your institution. Similarly, when contacting potential participants by telephone, do not disclose the personal information of the potential participant by identifying your institution or the purpose of the telephone call in a voice mail message, a message left on an answering machine, or a message taken by a third party who happens to answer the telephone. Also, steps should be taken to ensure that the name of your institution is not inadvertently disclosed to third parties through telecommunications technology such as Caller Identification.

Best Practice #22

When contacting potential survey participants, take steps to protect their privacy by not disclosing to third parties the name of your institution or the reason for contacting the potential survey participant.

Providing Assurances of Confidentiality

To encourage them to participate in the research and to provide open and honest responses, researchers typically assure survey research participants that their responses will be kept confidential. However, as previously noted, not all of the information provided by survey participants (e.g., the views and opinions expressed by individuals in their professional capacity) will be considered to be personal information that is subject to the privacy protection provisions of the *Acts*. In addition, all records (i.e., personal information and general records) in the custody or under the control of an institution could be subject to an access request under the *Acts*.

Regardless of whether the survey is conducted anonymously, the institution maintaining the information must assess whether it has the authority, under sections 41/31 of the *Acts*, to use the information to contact potential research participants (on behalf of the institution conducting the research).

Best Practice #19

If possible, avoid collecting personal information to obtain a survey research sample, by having the institution or third party that maintains the personal information contact potential research participants directly on your behalf.

Best Practice #20

Before using personal information to contact potential research participants on behalf of another institution or third party, assess whether you are authorized to use the information for this purpose, under sections 41/31 of the *Acts*.

Implications for Personal Information Banks

Regardless of whether notice was provided at the time of collection, if you use personal information to obtain a survey research sample, ensure that you comply with the requirements for personal information banks set out under sections 44 to 46 of the provincial *Act,* and sections 34 and 35 of the municipal *Act*. A *personal information bank* consists of personal information under your institution's control that is organized or intended to be retrieved by the individual's name or by an identifying number, symbol or other particular assigned to the individual.

If the personal information of customers or clients is to be used for survey research purposes on a regular basis, then this should be specified in the index of personal information banks, as required under subsections 45(d)/34(1)(d) of the *Acts*. Where the use has not been included in the index of personal information banks, sections 46(1)(a)/35(1)(a) of the *Act*s require that you attach or link to the personal information a record of this use. In addition, if the use has not been included in the index, section 46(3) of the provincial *Ac*t requires that the responsible minister be notified and the use be included in the index in the future. Under section 34(2) of the municipal *Act,* you must ensure that the index is amended as required to ensure its accuracy.

Best Practice #21

When using personal information to select a survey research sample, comply with the requirements for personal information banks set out under sections 44 to 46 of the provincial *Act*, or sections 34 and 35 of the municipal *Act*.

Stage 5: Data Collection

Contacting Potential Participants in the Survey

The fact that an individual has received one of your institution's programs or services could be considered to be sensitive personal information. When contacting potential survey participants, ensure that you do not invade their privacy by inadvertently disclosing this information to third parties, such as family members or co-workers.

For example, when contacting potential participants by mail, your institution name should not be printed on the outside of the envelope, as this information could reveal to others residing in the household that the individual has some relationship with your institution. Similarly, when contacting potential participants by telephone, do not disclose the personal information of the potential participant by identifying your institution or the purpose of the telephone call in a voice mail message, a message left on an answering machine, or a message taken by a third party who happens to answer the telephone. Also, steps should be taken to ensure that the name of your institution is not inadvertently disclosed to third parties through telecommunications technology such as Caller Identification.

Best Practice #22

When contacting potential survey participants, take steps to protect their privacy by not disclosing to third parties the name of your institution or the reason for contacting the potential survey participants.

Providing Assurances of Confidentiality

To encourage them to participate in the research and to provide open and honest responses, researchers typically assure survey research participants that their responses will be kept confidential. However, as previously noted, not all of the information provided by survey participants (e.g., the views and opinions expressed by individuals in their professional capacity) will be considered to be personal information that is subject to the privacy protection provisions of the *Acts*. In addition, all records (i.e., personal information and general records) in the custody or under the control of an institution could be subject to an access request under the *Acts*.

The only way to ensure complete confidentiality is to avoid collecting personal information altogether by conducting anonymous surveys. Where the research design, for one reason or another, requires that the survey data be linked to an individual, assurances of confidentiality should only be provided with the proviso that confidentiality is not absolute — that a disclosure of personal information may occur if required by statute.

Best Practice #23

Unless the survey is done anonymously, provide assurances of confidentiality only with the proviso that confidentiality is not absolute — that a disclosure of personal information may occur if required by statute.

Providing Notice of Collection

Unless the survey is conducted anonymously, notice of the collection of personal information should be provided at the time of the survey. The requirements for providing notice of collection are outlined in Stage 4.

Best Practice #24

When collecting personal information to conduct a survey, provide notice of collection, in compliance with sections 39(2)/29(2) of the *Acts*, unless a waiver has been obtained.

Obtaining Informed Consent

Participation in survey research should always be on a voluntary basis. Individuals should not be asked to participate without their informed consent. Regardless of whether the survey responses are anonymous or linked to an identifiable individual, potential participants should be provided with as much information about the survey as possible. For example, the information provided to potential research participants may include the following:

- the name of the organization conducting the research;
- the name of the institution sponsoring the research;
- the purpose of the research;
- how much time will be involved;
- that participation is voluntary and non-response to specific items is acceptable; and
- how respondents will be informed about the survey results.

In addition, if the survey is not being done anonymously, individuals should be told why it will be necessary to link the survey responses to personal information (i.e., to link survey responses with information collected at another point in time or with information obtained from another source such as a client or customer database, or to follow-up with participants on their specific responses to the survey).

Best Practice #25

Before collecting any information from potential survey participants, provide sufficient information about the research project and obtain informed consent.

Collecting Personal Information from Third Parties

In most survey research, any personal information that is collected will be collected directly from the individual to whom it relates. However, it is possible that some research designs may require the collection of personal information from third parties such as family members, caregivers, social workers, co-workers, or employees' supervisors.

Sections 39(1)/29(1) of the *Acts* require that personal information be collected directly from the individual to whom it relates, unless certain circumstances listed in sections 39(1)(a) to (h)/29(1)(a) to (h) exist (e.g., where the individual authorizes another manner of collection, where another manner of collection is authorized by or under a statute, etc.). Thus, if you intend to collect personal information from someone other than the individual to whom it relates, you must determine whether you have the authority to do so under sections 39(1)/29(1).

Best Practice #26

Whenever possible, collect personal information directly from the individual to whom it relates.

Best Practice #27

In conducting a survey in which personal information is to be collected from someone other than the individual to whom it relates, assess whether you have the authority to do so under sections 39(1)/29(1) of the *Acts*.

The only way to ensure complete confidentiality is to avoid collecting personal information altogether by conducting anonymous surveys. Where the research design, for one reason or another, requires that the survey data be linked to an individual, assurances of confidentiality should only be provided with the proviso that confidentiality is not absolute — that a disclosure of personal information may occur if required by statute.

[redacted]

Providing Notice of Collection

Unless the survey is conducted anonymously, notice of the collection of personal information should be provided at the time of the survey. The requirements for providing notice of collection are outlined in Stage 4.

[redacted]

Obtaining Informed Consent

Participation in survey research should always be on a voluntary basis. Individuals should not be asked to participate without their informed consent. Regardless of whether the survey responses are anonymous or linked to an identifiable individual, potential participants should be provided with as much information about the survey as possible. For example, the information provided to potential research participants may include the following:

- the name of the organization conducting the research;
- the name of the institution sponsoring the research;
- the purpose of the research;
- how much time will be involved;
- that participation is voluntary and non-response to specific items is acceptable; and
- how respondents will be informed about the survey results.

In addition, if the survey is not being done anonymously, individuals should be told why it will be necessary to link the survey responses to personal information (i.e., to link survey responses with information collected at another point in time or with information obtained from another source such as a client or customer database, or to follow-up with participants on their specific responses to the survey).

Best Practice #25

Before collecting any information from potential survey participants, provide sufficient information about the research project and obtain informed consent.

Collecting Personal Information from Third Parties

In most survey research, any personal information that is collected will be collected directly from the individual to whom it relates. However, it is possible that some research designs may require the collection of personal information from third parties such as family members, caregivers, social workers, co-workers, or employees' supervisors.

Sections 39(1)/29(1) of the *Acts* require that personal information be collected directly from the individual to whom it relates, unless certain circumstances listed in sections 39(1)(a) to (h)/29(1)(a) to (h) exist (e.g., where the individual authorizes another manner of collection, where another manner of collection is authorized by or under a statute, etc.). Thus, if you intend to collect personal information from someone other than the individual to whom it relates, you must determine whether you have the authority to do so under sections 39(1)/29(1).

[illegible]

[illegible]

Stage 6: Data Analysis

In analysing the data, the survey responses should only be used and disclosed for the purposes specified to the survey participants at the time of collection. Sections 41/31 of the *Acts* address the *use* of personal information. These sections state that an institution shall not use personal information in its custody or under its control except,

- where the person to whom the information relates has identified that information in particular and consented to its use;
- for the purpose for which it was obtained or compiled or for a consistent purpose; or
- for a purpose for which the information may be disclosed to the institution under sections 42/32 of the *Acts*.

If you decide to use or disclose the survey responses for a secondary purpose not specified at the time of collection and the survey has not been conducted anonymously, obtain the individual's consent.

Best Practice #10

[illegible] collected through the survey only for the purpose(s) specified to the survey participants at the time of collection.

[illegible]

[illegible]

Stage 7: Reporting of Results

Survey results are generally reported as aggregate information, thus protecting the privacy of individual participants. However, in some cases a survey may result in small cells of information (i.e., where a small number of people is being represented), that could inadvertently identify or be used to identify an individual. For example, in an anonymous survey of institution employees, survey participants might be asked to specify their gender and employee category (i.e., executive, manager, supervisor, or staff). But, if there is only one individual of a particular gender who falls within a particular employee category (e.g., female/executive), then that individual's responses will be easy to identify.

If it is known in advance that a survey could result in information that relates to a small number of individuals (i.e., small cells), the collection of personal information can be avoided by eliminating or combining those categories that include few individuals. In the above example, the size of the cells could be increased by eliminating gender categories or by combining executives and managers into one category. However, if the potential occurrence of small cells is not anticipated in advance and personal information is inadvertently collected, further use and disclosure of this information should be avoided by not reporting information relating to a small number of individuals (e.g., less than five).

Best Practice #30

Report survey results as aggregate information.

Best Practice #31

Don't report small cells of information where a specific individual could be identified.

Stage 8: Data Archiving

Institutions must consider how the survey data will be stored for future use, for how long and in what format it will be stored, and how it will eventually be disposed of. If the survey has not been done anonymously, there are certain requirements for retaining personal information specified in the *Acts*.

In addition to these requirements, whenever possible, all personal information should be replaced with a special code and stored separately from the survey responses. The survey responses should only be relinked to the personal information when it is necessary to do so for specific purposes.

With respect to disposal, all provincial government records are subject to the *Archives Act* and Management Board Directive 7-5, and may not be disposed of without the authorization of the Archivist of Ontario.

[illegible]

Stage 6: Data Analysis

In analysing the data, the survey responses should only be used and disclosed for the purposes specified to the survey participants at the time of collection. Sections 41/31 of the *Acts* address the *use* of personal information. These sections state that an institution shall not use personal information in its custody or under its control except,

- where the person to whom the information relates has identified that information in particular and consented to its use;
- for the purpose for which it was obtained or compiled or for a consistent purpose; or
- for a purpose for which the information may be disclosed to the institution under sections 42/32 of the *Acts*.

If you decide to use or disclose the survey responses for a secondary purpose not specified at the time of collection and the survey has not been conducted anonymously, obtain the individual's consent.

Best Practice #28

Use and disclose personal information collected through the survey only for the purpose(s) specified to the survey participants at the time of collection.

Best Practice #29

Before using personal information for a purpose not specified at the time of collection, obtain the individual's consent.

Stage 7: Reporting of Results

Survey results are generally reported as aggregate information, thus protecting the privacy of individual participants. However, in some cases a survey may result in small cells of information (i.e., where a small number of people is being represented), that could inadvertently identify or be used to identify an individual. For example, in an anonymous survey of institution employees, survey participants might be asked to specify their gender and employee category (i.e., executive, manager, supervisor, or staff). But, if there is only one individual of a particular gender who falls within a particular employee category (e.g., female/executive), then that individual's responses will be easy to identify.

If it is known in advance that a survey could result in information that relates to a small number of individuals (i.e., small cells), the collection of personal information can be avoided by eliminating or combining those categories that include few individuals. In the above example, the size of the cells could be increased by eliminating gender categories or by combining executives and managers into one category. However, if the potential occurrence of small cells is not anticipated in advance and personal information is inadvertently collected, further use and disclosure of this information should be avoided by not reporting information relating to a small number of individuals (e.g., less than five).

Best Practice #30

Report survey results as aggregate information.

Best Practice #31

Don't report small cells of information, where a specific individual could be identified.

Stage 8: Data Archiving

Institutions must consider how the survey data will be stored for future use, for how long and in what format it will be stored, and how it will eventually be disposed of. If the survey has not been done anonymously, there are certain requirements for retaining personal information specified in the *Acts*.

In addition to these requirements, whenever possible, all personal information should be replaced with a special code and stored separately from the survey responses. The survey responses should only be relinked to the personal information when it is necessary to do so for specific purposes.

With respect to disposal, all provincial government records are subject to the *Archives Act* and Management Board Directive 7-5, and may not be disposed of without the authorization of the Archivist of Ontario.

Best Practice #32

Whenever possible, replace personal information with a special code and store it separately from the survey responses.

Best Practice #33

Retain personal information for the period prescribed in the *Acts* (i.e., section 40(1) of the provincial *Act* together with section 5 of Regulation 460/section 30(1) of the municipal *Act* together with section 5 of Regulation 823).

Best Practice #34

Keep personal information secure as prescribed in the regulations (i.e., section 4 of Regulation 460/section 3 of Regulation 823).

Best Practice #35

To properly dispose of personal information, provincial institutions must comply with section 40(4) of the provincial *Act* together with Regulation 459 and with the *Archives Act* and Management Board Directive 7-5. Municipal institutions should follow the disposal procedures outlined in *IPC Practice 26, Safe and Secure Disposal Procedures for Municipal Institutions*, as there is no equivalent regulation under section 30(4) of the municipal *Act*.

Conclusion

Government institutions are more frequently undertaking survey research to elicit input on their programs and services. This paper has detailed the privacy considerations at each stage in the design and implementation of survey research projects, and has recommended some best practices.

Collecting personal information from survey participants, and using previously collected personal information to obtain a survey research sample are the two central privacy considerations in survey research. With respect to the collection of personal information, we support the view that most survey research can be carried out anonymously and personally identifiable survey data is only required in limited and specific circumstances. With respect to the use of previously collected personal information, even where survey research is carried out anonymously, personal information may still be needed to obtain your survey sample. Thus, you will need to consider individual privacy and compliance with the *Acts* in most cases.

Appendix A — Sample Terms of Reference

Whenever staff of an institution conduct survey research, Terms of Reference should set out the requirements for the collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. A sample Terms of Reference for a municipal institution is found below.

Terms of Reference

(Preamble describing events leading up to the survey, the survey itself, etc.)

- The purpose of this survey is to ____.
- The staff responsible for conducting the survey are ____________________________.
- The staff conducting the survey shall comply with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*, and its regulations, in the course of conducting the survey.
- The staff conducting the survey will use and/or disclose the data, information, reports, material or other documents of any nature which are disclosed, revealed or transmitted to them, or to which they have access, solely for the purpose of conducting the survey.
- Staff will collect, use or disclose only the minimal amount of personal information necessary to conduct the survey.
- When personal information is collected, staff shall provide the survey respondents with proper notice of collection, in accordance with section 29(2) of the *Municipal Freedom of Information and Protection of Privacy Act.*
- Staff will ensure that personal information used during the survey shall be retained in accordance with section 30(1) of the *Municipal Freedom of Information and Protection of Privacy Act* together with section 5 of Regulation 823.
- Staff will ensure that any personal information to be disposed of upon completion of the survey, is done so in accordance with the disposal procedures outlined in *IPC Practice 26, Safe and Secure Disposal Procedures for Municipal Institutions.*
- Staff shall keep all information involved in the survey secure and confidential.

For more information, contact: ____.

Appendix B — Sample Agreement with External Consultant

Where an external consultant or private company conducts the research, a contractual agreement should be established to ensure that personal information is collected, retained, used, disclosed and disposed of, in accordance with the *Acts*. A sample agreement of related terms and conditions for a provincial institution is found below.

- The Researcher agrees to comply with the provisions of the *Freedom of Information and Protection of Privacy Act*, and its regulations, in the course of providing Services pursuant to the Agreement.
- The Researcher agrees that it will use and/or disclose data, information, reports, material or other documents of any nature which are disclosed, revealed or transmitted to it by the Institution, or to which it or any of its employees have access, solely for the purpose of conducting the Survey.
- The Researcher agrees that, in conducting the Survey, only the minimal amount of personal information necessary will be collected, used or disclosed.
- The Researcher agrees that when it collects personal information, as defined in the *Freedom of Information and Protection of Privacy Act*, it shall provide the survey respondents with the proper notice of collection, in accordance with section 39(2) of the *Freedom of Information and Protection of Privacy Act*.
- The Researcher agrees that upon completion of the Survey or termination of the Agreement, all personal information collected, used or disclosed during the course of the Agreement will either be disposed of, in accordance with section 40(4) of the *Freedom of Information and Protection of Privacy Act* together with Regulation 459, or returned to the Institution by the date specified in the Agreement.
- The Researcher and the Institution agree that all records created or maintained in the course of providing Services pursuant to this Agreement become and remain the property of the Institution and that such records are or will be under the Institution's "control" within the meaning of section 10(1) of the *Freedom of Information and Protection of Privacy Act*.
- The Researcher agrees that all information involved in the Survey will be kept secure and confidential by the Researcher.

- If a request is made to the Researcher under the *Freedom of Information and Protection of Privacy Act* for access to records generated or maintained in the course of providing Services pursuant to this Agreement, within seven days of receipt of the request, the request must be directed to the Institution's Freedom of Information and Privacy Co-ordinator, together with copies of all responsive records in the custody or under the control of the Researcher.
- If a request is made to the Institution under the *Freedom of Information and Protection of Privacy Act* for access to records generated or maintained in the course of providing Services pursuant to this Agreement, within seven days of being directed to do so by the Institution, the Researcher must provide all responsive records in its custody or under its control to the Institution's Freedom of Information and Privacy Co-ordinator.
- The Researcher must designate a person to be responsible for records management, access to information and protection of privacy matters.

APPENDIX E

IPC's Proposed Amendments to the *Freedom of Information and Protection of Privacy Act* (Part IV)

- existing provisions shown in plain text
- new and amended provisions shown in bold text
- new and amended section headings underlined

PART IV

ADMINISTRATION AND ENFORCEMENT -- ss. 50 to 56

Right to appeal -- s. 50(1)

50. (1) A person who has made a request for,

(a) access to a record under subsection 24(1);

(b) access to personal information under subsection 48(1); or

(c) correction of personal information under subsection 47(2),

or a person who is given notice of a request under subsection 28(1) may appeal any decision of a head under this Act to the Commissioner.

Fee -- s. 50(1.1)

(1.1) A person who appeals under subsection (1) shall pay the fee prescribed by the regulations for that purpose.

Time for application -- s. 50(2)

(2) An appeal under subsection (1) shall be made within thirty days after the notice was given of the decision appealed from by filing with the Commissioner written notice of appeal.

Immediate dismissal -- s. 50(2.1)

(2.1) The Commissioner may dismiss an appeal if the notice of appeal does not present a reasonable basis for concluding that the record or the personal information to which the notice relates exists.

Non-application -- s. 50(2.2)

(2.2) If the Commissioner dismisses an appeal under subsection (2.1), subsection (3) and sections 51 and 52 do not apply to the Commissioner.

Notice of application for appeal -- s. 50(3)

(3) Upon receiving a notice of appeal, the Commissioner shall inform the head of the institution concerned and any other affected person of the notice of appeal. 1987, c. 25, s. 50(3).

***Ombudsman Act* not to apply -- s. 50(4) (Amended)**

(4) The *Ombudsman Act* does not apply in respect of a complaint for which an appeal, **compliance investigation or compliance audit** is provided under this Act or the *Municipal Freedom of Information and Protection of Privacy Act* or to the Commissioner or the Commissioner's delegate acting under this Act or the *Municipal Freedom of Information and Protection of Privacy Act*.

Mediator to try to effect settlement of appeal -- s. 51

51. The Commissioner may authorize a mediator to investigate the circumstances of any appeal and to try to effect a settlement of the matter under appeal. 1987, c. 25, s. 51.

Compliance investigations and audits -- s. 50.1 (New)

51.1. The Commissioner has the power to conduct investigations and audits to ensure compliance with any provision of this Act.

Notice of intention to investigate -- s. 50.2 (New)

51.2. Before commencing an investigation under this Act, the Commissioner shall notify the head of the institution concerned of the intention to carry out the investigation and of the substance of the investigation.

Mediator to try to effect settlement of complaint -- s. 51.1 (New)

51.3. Where the Commissioner receives a complaint from an individual concerning an issue of compliance with any provision of this Act that affects the individual, the Commissioner may authorize a mediator to investigate the complaint and try to effect a settlement of the matter.

Inquiry in appeal -- s. 52(1) (Amended)

52. (1) The Commissioner may conduct an inquiry, **in accordance with this section,** to review the head's decision if,

(a) the Commissioner has not authorized a mediator to conduct an investigation under section 51; or

(b) the Commissioner has authorized a mediator to conduct an investigation under section 51 but no settlement has been effected.

Inquiry in compliance investigation – **s. 52(1.1) (New)**

(1.1) The Commissioner may conduct a compliance investigation by way of inquiry, in accordance with this section, with respect to an issue of compliance with any provision of this Act,

(a) on receipt of a complaint from an individual concerning an issue of compliance with any provision of this Act that affects the individual, where,

(i) the Commissioner has not authorized a mediator to conduct an investigation under section 51.3; or

(ii) the Commissioner has authorized a mediator to conduct an investigation under section 51.3 but no settlement has been effected;

(b) on the request of the head of an institution concerning an issue of compliance with any provision of this Act that affects the institution; or

(c) where it appears to the Commissioner that an institution may not be in compliance with a provision of this Act.

Procedure -- s. 52(2) (Amended)

(2) The Statutory Powers Procedure Act does not apply to an inquiry under subsection (1) **or (1.1)**.

Inquiry in private -- s. 52(3)

(3) The inquiry may be conducted in private.

Powers of Commissioner -- s. 52(4)

(4) In an inquiry, the Commissioner may require to be produced to the Commissioner and may examine any record that is in the custody or under the control of an institution, despite Parts II and III of this Act or any other Act or privilege, and may enter and inspect any premises occupied by an institution for the purposes of the investigation.

Record not retained by Commissioner -- s. 52(5)

(5) The Commissioner shall not retain any information obtained from a record under subsection (4).

Examination on site -- s. 52(6)

(6) Despite subsection (4), a head may require that the examination of a record by the Commissioner be of the original at its site.

Notice of entry -- s. 52(7)

(7) Before entering any premises under subsection (4), the Commissioner shall notify the head of the institution occupying the premises of his or her purpose.

Examination under oath -- s. 52(8)

(8) The Commissioner may summon and examine on oath any person who, in the Commissioner's opinion, may have information relating to the inquiry, and for that purpose the Commissioner may administer an oath.

Evidence privileged -- s. 52(9)

(9) Anything said or any information supplied or any document or thing produced by a person in the course of an inquiry by the Commissioner under this Act is privileged in the same manner as if the inquiry were a proceeding in a court.

Protection -- s. 52(10)

(10) Except on the trial of a person for perjury in respect of his or her sworn testimony, no statement made or answer given by that or any other person in the course of an inquiry by the Commissioner is admissible in evidence in any court or at any inquiry or in any other proceedings, and no evidence in respect of proceedings before the Commissioner shall be given against any person.

Protection under Federal Act -- s. 52(11)

(11) A person giving a statement or answer in the course of an inquiry before the Commissioner shall be informed by the Commissioner of his or her right to object to answer any question under section 5 of the Canada Evidence Act.

Prosecution -- s. 52(12)

(12) No person is liable to prosecution for an offence against any Act, other than this Act, by reason of his or her compliance with a requirement of the Commissioner under this section.

Representations -- s. 52(13) (Amended)

(13) The person who requested access to the record **or the individual who made the complaint, as the case may be,** the head of the institution concerned and any affected party shall be given an opportunity to make representations to the Commissioner, but no person is entitled to be present during, to have access to or to comment on representations made to the Commissioner by any other person.

Right to counsel -- s. 52(14) (Amended)

(14) The person who requested access to the record **or the individual who made the complaint, as the case may be,** the head of the institution concerned and any affected party may be represented by counsel or an agent.

Burden of proof -- s. 53

53. Where a head refuses access to a record or a part of a record, the burden of proof that the record or the part falls within one of the specified exemptions in this Act lies upon the head. 1987, c. 25, s. 53.

Order in appeal -- s. 54(1) (Amended)

54. (1) After all of the evidence for an inquiry has been received, the Commissioner shall make an order disposing of the issues raised by the appeal **or considered in the investigation**.

Idem -- s. 54(2)

(2) Where the Commissioner upholds a decision of a head that the head may refuse to disclose a record or a part of a record, the Commissioner shall not order the head to disclose the record or part.

Order in compliance investigation -- s. 54(2.1) (New)

(2.1) Where an inquiry is in relation to an investigation, the Commissioner may, by order, do one or more of the following:

> **(a) require that a duty imposed by this Act be performed;**
>
> **(b) require an institution to cease collecting, using or disclosing personal information in contravention of this Act;**
>
> **(c) require an institution to destroy personal information collected or disclosed in contravention of this Act;**

(d) require an institution to change, cease or not commence an information practice specified by the Commissioner, if the Commissioner determines that the information practice contravenes this Act;

(e) require an institution to implement an information practice specified by the Commissioner, if the Commissioner determines that the information practice complies with this Act;

(f) require that, within a specified time, an institution give the Commissioner notice of any action to be taken or proposed to be taken to implement any recommendations that the Commissioner considers appropriate, or reasons why no such action has been or is proposed to be taken.

Terms and conditions -- s. 54(3)

(3) Subject to this Act the Commissioner's order may contain any terms and conditions the Commissioner considers appropriate.

Notice of order -- s. 54(4) (Amended)

(4) The Commissioner shall give the appellant and the persons who received notice of the appeal under subsection 50(3), **or, in the case of an investigation, the individual who made the complaint, the head of the institution concerned and any affected party,** written notice of the order.

Enforcement -- s. 54(5) (New)

(6) A copy of an order made by the Commissioner under this section, exclusive of the reasons therefor, may be filed with a clerk of the Superior Court of Justice, whereupon the order shall be entered in the same way as a judgment or order of that court and is enforceable as such.

Compliance Audit -- s. 54.1(2) (New)

54.1. (1) The Commissioner may, from time to time at the discretion of the Commissioner, carry out audits in respect of personal information and general records under the control of government institutions to ensure compliance with this Act.

Inquiry powers apply -- s. 54.1(2) (New)

(2) Sections 51.2 and 52 apply, where appropriate and with such modifications as the circumstances require, in respect of audits carried out under subsection (1).

Report of findings and recommendations -- s. 54.1(3) (New)

(3) If, following an audit under subsection (1), the Commissioner considers that an institution has not complied with the Act, the Commissioner shall provide the head of the institution with a report containing the findings of the audit and any recommendations that the Commissioner considers appropriate.

Idem -- s. 54.1(4) (New)

(4) Where the Commissioner makes a report under subsection (3), the Commissioner may require that, within a specified time, an institution give the Commissioner notice of any action to be taken or proposed to be taken to implement the recommendations or reasons why no such action has been or is proposed to be taken.

Confidentiality -- s. 55(1)

55. (1) The Commissioner or any person acting on behalf of or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their powers, duties and functions under this or any other Act.

Not compellable witness -- s. 55(2)

(2) The Commissioner or any person acting on behalf or under the direction of the Commissioner is not compellable to give evidence in a court or in a proceeding of a judicial nature concerning anything coming to their knowledge in the exercise or performance of a power, duty or function under this or any other Act.

Proceedings privileged -- s. 55(3)

(3) No proceeding lies against the Commissioner or against any person acting on behalf or under the direction of the Commissioner for anything done, reported or said in good faith in the course of the exercise or performance or intended exercise or performance of a power, duty or function under this or any other Act.

Delegation by Commissioner -- s. 56(1)

56. (1) The Commissioner may in writing delegate a power or duty granted to or vested in the Commissioner to an officer or officers employed by the Commissioner, except the power to delegate under this section, subject to such limitations, restrictions, conditions and requirements as the Commissioner may set out in the delegation.

Exception re records under s. 12 or 14 -- s. 56(2)

(2) The Commissioner shall not delegate to a person other than an Assistant Commissioner his or her power to require a record referred to in section 12 or 14 to be produced and examined.

Note: Consequential amendments to section 59(b) [repealed] and otherwise in the Act may be necessary to implement the letter and spirit of these amendments.

Note: Equivalent amendments are proposed in relation to the *Municipal Freedom of Information and Protection of Privacy Act*